CONVENIO SOBRE LA CIBERDELINCUENCIA

(STE núm. 185)

Informe explicativo

I. El Convenio y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001) y el Convenio fue abierto a la firma en Budapest, el 23 de noviembre de 2001, con motivo de la celebración de la Conferencia Internacional sobre la ciberdelincuencia.

II. El texto de este informe explicativo no constituye un instrumento que ofrezca una interpretación autorizada del Convenio, aunque por su naturaleza tal vez facilite la aplicación de las disposiciones contenidas en el mismo.

I. Introducción

1. La revolución de las tecnologías de la información ha modificado radicalmente a la sociedad y probablemente seguirá haciéndolo en un futuro cercano. Muchas tareas son más fáciles de realizar. Si bien en un principio sólo algunos sectores específicos de la sociedad habían racionalizado sus procedimientos de trabajo con la ayuda de la tecnología de la información, en la actualidad se ven afectados casi todos los sectores de la sociedad. La tecnología de la información, de un modo o de otro, ha invadido casi todos los aspectos de las actividades humanas.

2. Una característica notable de la tecnología de la información es el impacto que ha tenido, y que tendrá, en la evolución de la tecnología de las telecomunicaciones. La telefonía clásica, que supone la transmisión de la voz humana, se ha visto superada por el intercambio de grandes cantidades de datos, que incluyen voz, texto, música e imágenes estáticas y en movimiento. Este intercambio ya no ocurre sólo entre los seres humanos, sino también entre los seres humanos y los ordenadores, y entre los mismos ordenadores. Las redes de conmutación de circuitos han sido reemplazadas por redes de conmutación de paquetes. Ya no es relevante si se puede establecer o no una conexión directa; basta con ingresar los datos en una red con una dirección de destino o ponerlos a disposición de cualquiera que quiera acceder a los mismos.

3. El uso generalizado del correo electrónico y del acceso por Internet a numerosos sitios web son ejemplos de esta evolución. Nuestra sociedad ha sufrido cambios profundos.

4. La facilidad para buscar y acceder a la información contenida en los sistemas informáticos, unida a las posibilidades casi ilimitadas para su intercambio y difusión, sin tener en cuenta las distancias geográficas, ha conducido a un crecimiento explosivo en la cantidad de información disponible y de los conocimientos que se pueden extraer de la misma.

5. Estos acontecimientos han dado lugar a cambios económicos y sociales sin precedentes, pero también tienen un lado oscuro: el surgimiento de nuevos tipos de delitos, así como también la comisión de delitos tradicionales mediante el uso de las nuevas tecnologías. Por otra parte, las consecuencias del comportamiento delictivo pueden tener mayor alcance que antes, porque no están restringidas por los límites geográficos o las fronteras nacionales. La reciente propagación de virus informáticos nocivos por todo el mundo es un buen ejemplo de esta realidad. Es necesario aplicar medidas técnicas con el fin de proteger los sistemas informáticos, al mismo tiempo que se adoptan medidas jurídicas destinadas a prevenir e impedir los comportamientos delictivos.

6. Las nuevas tecnologías constituyen un desafío para los conceptos jurídicos existentes. La información y la comunicación fluyen con mayor facilidad por todo el mundo. Las fronteras han dejado de ser barreras para ese flujo. Los delincuentes se encuentran cada vez menos en los lugares en que se hacen sentir los efectos de sus actos. Sin embargo, la legislación nacional está confinada generalmente a un territorio específico. Es por ello que las soluciones a los problemas planteados deben ser abordadas por el derecho internacional, lo que requiere la adopción de instrumentos jurídicos internacionales adecuados. El presente Convenio tiene por objeto hacer frente a este desafío, con el debido respeto de los derechos humanos en la nueva Sociedad de la Información.

II. Trabajo preparatorio

7. Por decisión CDPC/103/211196, el Comité europeo para los problemas criminales (CDPC) decidió en noviembre de 1996 establecer un comité de expertos encargado de los delitos informáticos. El CDPC basó su decisión en la siguiente razón fundamental:

8. "Los rápidos desarrollos en el campo de la tecnología de la información influyen directamente sobre todos los sectores de la sociedad moderna. La integración de los sistemas de telecomunicaciones y de información, que posibilitan el almacenamiento y la transmisión de todo tipo de comunicaciones, sin tener en cuenta la distancia, crea una amplia gama de nuevas posibilidades. Estos desarrollos se vieron potenciados por la aparición

de las redes y las superautopistas de la información, incluida Internet, a través de las cuales prácticamente todas las personas pueden tener acceso a cualquier servicio de información electrónica, sin importar en qué lugar del mundo se encuentre. Al conectarse con los servicios de comunicaciones y de información, los usuarios crean una especie de espacio común, denominado "ciberespacio", que es utilizado con fines legítimos, pero que también puede ser objeto de un uso impropio. Estos "delitos cometidos en el ciberespacio" abarcan tanto actividades que atentan contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones como el uso de esas redes o sus servicios para cometer delitos tradicionales. El carácter transfronterizo de dichos delitos, por ej., cuando se cometen a través de Internet, está en conflicto con la territorialidad de las autoridades nacionales encargadas de imponer el cumplimiento de las leyes.

9. Por consiguiente, el derecho penal debe mantenerse al corriente de estos desarrollos tecnológicos que ofrecen oportunidades muy sofisticadas para hacer un mal uso de las facilidades del ciberespacio y perjudicar intereses legítimos. Dada la naturaleza transfronteriza de las redes de información, es necesario un esfuerzo internacional concertado para hacer frente a ese uso impropio. Si bien la Recomendación núm (89) 9 llevó a cierto grado de aproximación de los conceptos nacionales con respecto a ciertas formas de usos impropios de la informática, únicamente un instrumento internacional de carácter vinculante puede asegurar la eficacia necesaria en la lucha contra estos nuevos fenómenos. En el marco de dicho instrumento, además de las medidas de cooperación internacional, se deberían abordar las cuestiones de derecho sustantivo y procesal, así como cuestiones que están estrechamente relacionadas con el uso de la tecnología de la información".

10. Por otra parte, el CDPC tuvo en cuenta el Informe preparado, atendiendo a su pedido, por el profesor H.W.K. Kaspersen, que llegaba a la conclusión de que "... habría que buscar otro instrumento jurídico más obligatorio que una recomendación, tal como un convenio. Dicho convenio no debería abordar tanto las cuestiones de derecho penal sustantivo como las cuestiones de derecho procesal penal, así como también los acuerdos y procedimientos del derecho penal internacional".[1] Se había llegado a una conclusión similar en el informe adjunto a la Recomendación núm. R (89) 9[2], concerniente al derecho sustantivo, y la Recomendación núm. R (95) 13[3], relativa a los problemas de derecho procesal en relación con la tecnología de la información.

11. El mandato específico del nuevo comité fue el siguiente:

---

[1] Aplicación de la Recomendación núm. R (89) 9 sobre delitos informáticos, Informe preparado por el Profesor Dr. H.W.K. Kaspersen (doc. CDPC (97) 5 y PC-CY (97) 5, página 106).

[2] Véase *La delincuencia informática*, Informe del Comité Europeo para los Problemas Criminales, página 86.

[3] Véase *Los Problemas del derecho procesal penal relacionados con la tecnología de la información*, Recomendación núm. R (95) 13, principio núm. 17.

i. "Examinar, a la luz de las Recomendaciones núm. R (89) 9 sobre la delincuencia relacionada con la informática, y núm. R (95) 13, relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información, en particular los siguientes temas:

ii. Los delitos cometidos en el ciberespacio, en particular los cometidos mediante el uso de las redes de telecomunicaciones, por ej., Internet, tales como las transacciones ilegales de fondos, las ofertas de servicios ilegales, las infracciones de la propiedad intelectual, así como también los delitos que atentan contra la dignidad humana y la protección de los menores;

iii. otras cuestiones de derecho penal sustantivo donde puede ser necesario un enfoque común a los fines de lograr una cooperación internacional tales como las definiciones, las sanciones y la responsabilidad de las personas activas en el ciberespacio, incluidos los proveedores de servicios de Internet;

iv. el uso, incluida la posibilidad del uso transfronterizo y la aplicabilidad de los poderes coercitivos en un entorno tecnológico, por ej., la interceptación de telecomunicaciones y la vigilancia electrónica de las redes de información, por ej,, a través de Internet, el registro y la confiscación de datos almacenados en los sistemas de procesamiento de información (incluidos los sitios de Internet), la prohibición de acceder a material ilegal y el requerimiento de que los proveedores de servicios cumplan con obligaciones especiales, teniendo en cuenta los problemas causados por ciertas medidas de seguridad de la información como, por ej., el cifrado;

v. la cuestión de la jurisdicción en relación con los delitos relacionados con la tecnología de la información, por ej., el determinar el lugar donde se cometió un delito (*locus delicti*) y cuál es el derecho que corresponde aplicar, incluido el problema de *ne bis in idem* en el caso de múltiples jurisdicciones y la cuestión de cómo resolver los conflictos de jurisdicción positiva y la forma de evitar conflictos de jurisdicción negativa;

vi. cuestiones relativas a la cooperación internacional en la investigación de los delitos en el ciberespacio, en estrecha cooperación con el Comité de Expertos sobre el Funcionamiento de los Convenios Europeos en el Campo Penal (PC-OC).

El Comité elaborará el borrador de un instrumento jurídicamente vinculante, en la medida de lo posible, que abarque los incisos i) a v), poniendo particular énfasis en las cuestiones internacionales y, de ser apropiado, en las recomendaciones accesorias respecto de problemas específicos. El Comité puede formular sugerencias sobre otras cuestiones relacionadas con los desarrollos tecnológicos".

12. A raíz de la decisión del CDPC, el Comité de Ministros estableció el nuevo comité denominado "Comité de Expertos en la Delincuencia del Ciberespacio (PC-CY)" por decisión núm. CM/Del/Dec(97)583, adoptada en la 583a

reunión de los Ministros (celebrada el 4 de febrero de 1997). El Comité PC-CY inició su labor en abril de 1997 y llevó a cabo negociaciones acerca del proyecto de un convenio internacional sobre la ciberdelincuencia. Conforme a los términos de referencia originales, el Comité debía terminar su trabajo para el 31 de diciembre de 1999. Como para ese entonces el Comité no se encontraba en posición de concluir totalmente sus negociaciones sobre ciertas cuestiones incluidas en el proyecto del Convenio, sus términos de referencia se prorrogaron hasta el 31 de diciembre 2000 por la Decisión núm. CM/Del/Dec(99)679, de los Representantes de los Ministros. Los Ministros de Justicia europeos manifestaron su respaldo a las negociaciones en dos oportunidades mediante la Resolución núm. 1, aprobada en su 21ª Conferencia (Praga, junio de 1997), que recomendaba al Comité de Ministros que apoyara el trabajo llevado a cabo por el CDPC respecto de la ciberdelincuencia con el fin de lograr que las disposiciones internas en materia de derecho penal llegasen a ser lo más parecidas posibles entre sí, y de posibilitar el uso de medios eficaces de investigación en cuanto a dichos delitos. Reiteraron su respaldo en la Resolución núm. 3, aprobada en la 23ª Conferencia de Ministros de Justicia europeos (Londres, junio de 2000), que alentaba a las Partes negociadoras a proseguir sus esfuerzos con vistas a encontrar soluciones apropiadas para hacer posible que el mayor número posible de Estados llegasen a ser Partes del Convenio y reconocía la necesidad de contar con un sistema de cooperación internacional rápido y eficiente, que tuviera en cuenta debidamente las necesidades específicas que lleva aparejada la lucha contra la ciberdelincuencia. Los Estados miembros de la Unión Europea expresaron su apoyo a la labor realizada por el PC-CY, recogido en una Opinión Conjunta adoptada en mayo de 1999.

13. Entre abril de 1997 y diciembre de 2000, tuvieron lugar 10 reuniones plenarias del Comité PC-CY y 15 reuniones de su Grupo de Redacción. Al término de la extensión de su mandato, los expertos celebraron, bajo la tutela del CDPC, tres reuniones adicionales para finalizar el proyecto del Memorando Explicativo y volver a analizar el proyecto del Convenio a la luz de la opinión de la Asamblea Parlamentaria. En octubre de 2000, el Comité de Ministros solicitó a la Asamblea que emitiera un dictamen sobre el proyecto de Convenio, que fue adoptado en la segunda parte de su sesión plenaria en abril de 2001.

14. Con arreglo a una decisión tomada por el Comité PC-CY, una primera versión del proyecto de Convenio fue desclasificada y publicada en abril de 2000, que fue seguida de versiones posteriores publicadas al término de cada reunión plenaria, con el fin de posibilitar que los Estados negociadores pudieran efectuar consultas con todas las partes interesadas. Este proceso de consulta resultó muy útil.

15. El proyecto del Convenio revisado y finalizado y su Memorando Explicativo fueron sometidos para su aprobación al CDPC en su 50a sesión plenaria en junio de 2001, después de lo cual el texto del proyecto de

Convenio fue sometido al Comité de Ministros para su aprobación y quedó abierto para su firma.

III. El Convenio

16. El Convenio tiene como finalidad primordial: 1) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos; 2) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico, 3) establecer un régimen rápido y eficaz de cooperación internacional.

17. En consecuencia, el Convenio tiene cuatro capítulos: I) Terminología, II) Medidas que deberán adoptarse a nivel nacional – el derecho penal sustantivo y el derecho procesal, (III) Cooperación internacional y (IV) Cláusulas finales.

18. La Sección 1 del Capítulo II (Derecho penal sustantivo) abarca las disposiciones relativas a los delitos y otras disposiciones conexas referentes al ámbito de los delitos informáticos o los delitos relacionados con el empleo de ordenadores. En primer lugar, define 9 delitos agrupados en 4 categorías diferentes y más tarde versa sobre las responsabilidades y sanciones conexas. El Convenio define los siguientes delitos: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

19. La sección 2 (Derecho procesal) del capítulo II -- cuyo alcance va más allá de los delitos definidos en la Sección 1, ya que se aplica a cualquier delito cometido por medio de un sistema informático o a las pruebas que se encuentren en formato electrónico -- determina en primer lugar las condiciones y salvaguardias comunes aplicables a todos las facultades procesales contenidas en ese Capítulo. A continuación, establece los siguientes poderes procesales: conservación rápida de datos informáticos almacenados; conservación y revelación parcial rápidas de los datos relativos al tráfico; la orden de presentación; el registro y la confiscación de datos informáticos almacenados; la obtención en tiempo real de datos relativos al tráfico, y la interceptación de datos relativos al contenido. La última sección del Capítulo II incluye disposiciones en materia de jurisdicción.

20. El capítulo III contiene las disposiciones relativas a la asistencia mutua en relación con los delitos tradicionales y con los delitos relacionados con la informática, así como también las referentes a la extradición. Da cuenta de la

asistencia mutua tradicional en dos situaciones: cuando entre las partes no existen fundamentos jurídicos (tratados, leyes de reciprocidad, etc.) -- en cuyo caso corresponde aplicar sus disposiciones -- y cuando existe dicha base -- en cuyo caso los acuerdos existentes también se aplican a la asistencia que se concede en virtud del presente Convenio. La asistencia específica en materia de delitos informáticos o de delitos relacionados con la informática se aplica a ambas situaciones y abarca, sujeto a condiciones adicionales, la misma serie de facultades procesales definidas en el Capítulo II. Por otra parte, el Capítulo III contiene una disposición acerca de un tipo específico de acceso transfronterizo a datos informáticos almacenados, que no requiere la asistencia mutua (cuando media un consentimiento o cuando están disponibles públicamente) y prevé el establecimiento de una red que funcione las 24 horas del día los 7 días de la semana con el fin de asegurar una asistencia rápida entre las Partes.

21. Por último, el Capítulo IV contiene las disposiciones finales, las cuales -- con ciertas excepciones – recogen las disposiciones habituales de los tratados del Consejo de Europa.

Comentario sobre los artículos del Convenio

Capítulo I – Terminología

Introducción a las definiciones del Artículo 1

22. Quienes redactaron el Convenio entendieron que conforme al presente Convenio las Partes no estarían obligadas a copiar literalmente en su derecho interno los cuatro conceptos definidos en el Artículo 1, siempre que sus leyes abarcaran dichos conceptos de manera coherente con los principios del Convenio y ofrecieran un marco equivalente para su aplicación.

Artículo 1.a) - Sistema informático

23. A los efectos de este Convenio, un "sistema informático" es un dispositivo que consta de hardware y software cuya función es el tratamiento automatizado de datos digitales. Puede incluir facilidades de entrada (*input*), salida (*output*) y almacenamiento. Puede funcionar en forma independiente o estar conectado a una red con otros dispositivos similares. "Automatizado" significa sin intervención directa de un ser humano; "tratamiento de datos" significa que los datos que se encuentran en un sistema informático son operados mediante la ejecución de un programa informático. Un "programa informático" es un conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar el resultado deseado. Un equipo puede ejecutar diversos programas. Un sistema informático por lo general consta de diferentes dispositivos, diferenciándose entre el procesador o unidad de

procesamiento central y los periféricos. Un "periférico" es un dispositivo que realiza ciertas funciones específicas interactuando con la unidad de procesamiento, como puede ser una impresora, una pantalla de video, un dispositivo para leer o escribir CD u otros dispositivos de almacenamiento de datos.

24. Una red es una interconexión entre dos o más sistemas informáticos. Las conexiones pueden ser terrestres (por ej., alámbricas o por cable), inalámbricas (por ej., radioeléctricas, infrarrojas o satelitales), o de ambos tipos. Una red puede estar limitada geográficamente a un área pequeña (redes de área local) o puede abarcar un área extensa (redes de área extensa), y esas redes pueden a su vez estar interconectadas. Internet es una red global que consta de muchas redes interconectadas que utilizan protocolos comunes. Existen también otros tipos de redes, estén o no conectadas a Internet, capaces de transmitir datos informáticos entre sistemas informáticos. Los sistemas informáticos pueden estar conectados a la red como nodos o pueden ser un instrumento para brindar asistencia en la comunicación a través de la red. Lo esencial es el intercambio de datos a través de la red.

Artículo 1.b) - Datos informáticos

25. La definición de “datos informáticos” se basa en la definición de datos de la ISO. Esta definición contiene las palabras "que se preste a tratamiento informático". Esto significa que los datos están en un formato tal que pueden ser procesados directamente por un sistema informático. Con el fin de aclarar que en el presente Convenio el término “datos” debe entenderse como datos en formato electrónico u otro formato que se preste a tratamiento informático directamente, se introduce el concepto de "datos informáticos". Los datos informáticos que se procesan automáticamente pueden ser objeto de uno de los delitos definidos en el presente Convenio, así como el objeto de la solicitud de una de las medidas de investigación definidas en el presente Convenio.

Artículo 1.c) - Proveedor de servicios

26. El término "proveedor de servicios" abarca a una amplia categoría de personas que desempeñan un papel particular con respecto a la comunicación o el tratamiento de los datos a través de los sistemas informáticos (véanse también los comentarios correspondientes a la Sección 2). En el inciso i) de la definición, se aclara que quedan comprendidas todas las entidades tanto públicas como privadas que ofrecen a los usuarios la posibilidad de comunicarse entre sí. Por lo tanto, es irrelevante el hecho de que los usuarios constituyan un grupo cerrado, o que el proveedor ofrezca sus servicios al público, tanto gratuitamente como a cambio de un arancel.

Un grupo cerrado puede ser, por ej., los empleados de una empresa privada que reciben el servicio a través de la red de la empresa.

27. En el inciso ii) de la definición se aclara que el término "proveedor de servicios" abarca también a aquellas entidades que procesen o almacenen datos en nombre de las personas mencionadas en el inciso i). Además, el término abarca las entidades que almacenan o procesan datos en nombre de los usuarios de los servicios de las personas mencionadas en el inciso i). Por ejemplo, en virtud de esta definición, el término "proveedor de servicios" incluye tanto los servicios que proporcionan hospedaje (*hosting*) como los que ponen copias de los contenidos de los sitios web en dispositivos de almacenamiento temporal (*caching*), y también los servicios que proveen la conexión a una red. Sin embargo, esta definición no incluye a un mero proveedor de contenidos (tal como la persona que firma un contrato con una empresa de hospedaje de dominios (*web hosting*) para alojar su sitio web) si dicho proveedor de contenidos no ofrece también servicios de comunicaciones o servicios relacionados con el procesamiento de datos.

Artículo 1.d) - Datos relativos al tráfico

28. A los efectos del presente Convenio, los "datos relativos al tráfico" tal como se definen en el Artículo 1, acápite d), constituyen una categoría separada de datos informáticos que está sujeto a un régimen jurídico específico. Estos datos son generados por los ordenadores en la cadena de comunicación con el fin de encaminar una comunicación desde su punto de origen hasta su destino. Por tanto, son datos auxiliares a la comunicación misma.

29. En el caso de la investigación de un delito penal cometido en relación con un sistema informático, los datos relativos al tráfico son necesarios para rastrear el origen de una comunicación como punto de partida para reunir otras pruebas, o como parte de las pruebas del delito. Los datos relativos al tráfico podrían tener sólo una duración efímera, lo que hace necesario ordenar su rápida conservación. En consecuencia, su rápida revelación puede ser necesaria para averiguar la ruta de una comunicación, a fin de obtener otras pruebas antes de que sean eliminadas o para identificar a un sospechoso. Por lo tanto, el procedimiento ordinario para la obtención y revelación de los datos informáticos podría ser insuficiente. Además, la obtención de estos datos se considera, en principio, menos intrusiva ya que, como tal, no revela el contenido de la comunicación, que es considerado más sensible.

30. La definición enumera de forma exhaustiva las categorías de datos relativos al tráfico que están comprendidos bajo un régimen específico en el presente Convenio: el origen de una comunicación, su destino, la ruta, la hora (GMT), la fecha, el tamaño, la duración y el tipo de servicio subyacente. No todas esas categorías estarán siempre disponibles técnicamente, o podrán

ser suministradas por un proveedor de servicios, o serán necesarias para una investigación penal en particular. El "origen" se refiere a un número de teléfono, dirección de Protocolo de Internet (IP), o a una identificación similar de una instalación de comunicaciones a la que un proveedor de servicios presta sus servicios. El "destino" se refiere a una indicación comparable de una instalación de comunicaciones a las que se transmiten las comunicaciones. El término "tipo de servicio subyacente" se refiere al tipo de servicio que está siendo utilizado en la red, por ej., transferencia de archivos, correo electrónico o envío de mensajes instantáneos.

31. La definición deja a las legislaturas de cada país la posibilidad de introducir algún grado de diferenciación respecto de la protección legal de los datos relativos al tráfico de acuerdo con su sensibilidad. En este contexto, el Artículo 15 obliga a las Partes a establecer las condiciones y salvaguardias adecuadas para la protección de los derechos y las libertades humanas. Esto implica, entre otras cosas, que los criterios sustantivos y los procedimientos que corresponda aplicar conforme a una facultad de investigación pueden variar de acuerdo con la sensibilidad de los datos.

Capítulo II - Medidas que deberán adoptarse a nivel nacional

32. El Capítulo II (Artículos 2 a 22) contiene tres secciones: derecho penal sustantivo (artículos 2 a 13); derecho procesal (artículos 14 a 21) y jurisdicción (artículo 22).

Sección 1 - Derecho penal sustantivo

33. La Sección 1 del Convenio (Artículos 2 a 13) tiene como finalidad mejorar los medios para prevenir y evitar los delitos informáticos o los delitos relacionados con la informática al establecer una norma mínima común en relación con los delitos pertinentes. Este tipo de armonización facilita la lucha contra tales delitos en los ámbitos nacional e internacional. Si existen correspondencias entre las distintas leyes nacionales se pueden evitar abusos tales como el traslado del proceso a una Parte que aplique normas anteriores y sanciones menores. Por consiguiente, podría mejorar también el intercambio de experiencias comunes útiles en el manejo práctico de los casos. La cooperación internacional (especialmente la extradición y la asistencia judicial recíproca) se ve facilitada, por ej., respecto de los requisitos de doble tipificación penal.

34. La enumeración de los delitos incluidos representa un consenso mínimo, y no excluye las extensiones que puedan efectuarse en las leyes nacionales de cada una de las Partes. Se basa en gran medida en las directrices desarrolladas en relación con la Recomendación núm. R(89)9 del Consejo de Europa sobre delitos relacionados con el empleo de ordenadores y en el trabajo de otras organizaciones internacionales de carácter público o privado

(OCDE, Naciones Unidas, AIDP) , pero tiene en cuenta las experiencias más modernas con abusos cometidos debido a la expansión de las redes de telecomunicaciones.

35. La sección está dividida en cinco títulos. El Título 1 incluye los principales delitos informáticos: los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que constituyen las amenazas básicas, tal como fueron identificadas en los debates sobre la seguridad de los datos y los sistemas informáticos, y los riesgos a los que están expuestos el tratamiento electrónico de datos y los sistemas de comunicaciones. El título describe el tipo de delitos que abarca, que es el acceso no autorizado a sistemas, programas o datos y la manipulación ilícita de dichos sistemas, programas o datos. Los títulos 2 a 4 incluyen otros tipos de "delitos informáticos", que desempeñan un papel más importante en la práctica y en los que los sistemas informáticos y de telecomunicaciones son utilizados como medio para atacar ciertos intereses legales la gran mayoría de los cuales ya están protegidos por el derecho penal contra los ataques que utilizan medios tradicionales. Los delitos que abarca el Título 2 (falsificación y fraude informáticos) han sido agregados siguiendo las sugerencias incluidas en los lineamientos de la Recomendación núm. R(89)9 del Consejo de Europa. El Título 3 abarca los "delitos relacionados con el contenido" de la producción o distribución ilícita de pornografía infantil mediante el uso de sistemas informáticos, que es uno de los más peligrosos *modi operandi* en los últimos tiempos. El comité encargado de redactar el Convenio discutió la posibilidad de incluir otros delitos relacionados con los contenidos, tales como la distribución de propaganda racista a través de sistemas informáticos. Sin embargo, el Comité no pudo llegar a consenso con respecto a que dichas conductas constituyen un delito. Si bien hubo considerable respaldo para incluir ese tema como un delito penal, algunas delegaciones expresaron su profunda preocupación respecto de la inclusión de una disposición tal basándose en el derecho a la libertad de expresión. En vista de la complejidad de la cuestión, se decidió que el comité referiría al Comité europeo para los problemas criminales *(*CDPC*)* la cuestión de elaborar un Protocolo adicional al presente Convenio.

El Título 4 establece los "delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines". Estos fueron incluidos en el Convenio porque las infracciones de la propiedad intelectual son una de las formas más difundidas de delitos informáticos o de delitos relacionados con el empleo de ordenadores y su escalada es motivo de preocupación a nivel internacional. Por último, el Título 5 incluye disposiciones adicionales respecto de la tentativa, la complicidad y la instigación, así como las sanciones y medidas; asimismo aborda, al igual que otros recientes instrumentos internacionales, la cuestión de la responsabilidad de las personas jurídicas.

36. Si bien las disposiciones del derecho sustantivo se refieren a delitos que utilizan la tecnología de la información, el Convenio utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el

derecho penal puedan aplicarse a tanto a las tecnologías actuales como a las futuras.

37. Los encargados de redactar el Convenio entendieron que las Partes pueden excluir conductas indebidas de poca monta o insignificantes de la aplicación de los delitos contemplados en los Artículos 2 a 10.

38. Una particularidad de los delitos incluidos es el requisito expreso de que la conducta en cuestión sea llevada a cabo de manera "ilegítima". Esto refleja la idea de que la conducta descrita no siempre es punible *per se*, sino que puede ser legal o justificada, no sólo en aquellos casos en que corresponde aplicar una defensa legal clásica, como el consentimiento, la defensa propia o la necesidad, sino también cuando otros principios o intereses conducen a la exclusión de la responsabilidad penal. El término "ilegítimo" deriva su significado del contexto en que está utilizado. Así, sin restringir la manera en que las Partes pueden aplicar el concepto en su derecho interno, puede referirse a una conducta realizada sin facultades para hacerlo (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o a una conducta que no está de otro modo comprendida dentro de las justificaciones, excusas y defensas legales establecidas o los principios pertinentes con arreglo a las leyes nacionales. Por consiguiente, el Convenio no afecta a las conductas legítimas de un gobierno (por ej., cuando el gobierno de una de las Partes interviene para mantener el orden público, proteger la seguridad nacional o investigar delitos penales). Por otra parte, las actividades legítimas y comunes inherentes al diseño de las redes, o legítimas y comunes respecto de las prácticas comerciales no deben ser consideradas delitos. Ejemplos específicos de esos tipos de excepciones se presentan en relación con delitos específicos en el texto correspondiente del Memorando Explicativo que figura más abajo. Queda a criterio de las Partes determinar la manera en que esas exenciones son implementadas en sus sistemas jurídicos nacionales (conforme al derecho penal o de algún otro modo).

39. Todos los delitos contenidos en el Convenio deben ser cometidos de manera "deliberada" para que se aplique la responsabilidad penal. En ciertos casos un elemento deliberado específico forma parte del delito. Por ejemplo, en el Artículo 8 que trata del delito de fraude informático, la intención de obtener un beneficio económico es un elemento constitutivo del delito. Quienes redactaron el Convenio llegaron al acuerdo de que el significado exacto del término "deliberado" debería ser interpretado conforme a las leyes de cada país.

40. Ciertos artículos de la sección permiten añadir matizaciones a la hora de aplicar el Convenio en el derecho interno de cada país. En otros casos, se otorga incluso la posibilidad de formular una reserva (véanse los Artículos 40 y 42). Estas diferentes maneras de aplicar un enfoque más restrictivo por lo que se refiere a la penalización reflejan diferentes evaluaciones respecto de la peligrosidad del comportamiento involucrado o de la necesidad de usar el

derecho penal como contramedida. Este enfoque brinda flexibilidad a los gobiernos y parlamentos para determinar su política penal en este campo.

41. Las leyes que establecen estos delitos deberían ser redactadas con la mayor claridad y especificidad posible, con el fin de prever adecuadamente los tipos de conducta pasibles de una sanción penal.

42. En el transcurso del proceso de redacción, los encargados de la misma consideraron la conveniencia de establecer como delitos otras conductas además de las definidas en los Artículos 2 a 11, incluida la denominada "ciberocupación" (*cyber-squatting*), es decir, el hecho de registrar un nombre de dominio que sea idéntico al nombre de una entidad ya existente y que tiene en general cierto renombre o al nombre comercial o a la marca de un producto o empresa. Los ciberocupas (*cyber-squatters*) ilegales no tienen ninguna intención de hacer uso realmente del nombre de dominio y buscan obtener un beneficio financiero obligando a la entidad involucrada, aunque sea de forma indirecta, a pagar por la transferencia de la titularidad del nombre de dominio. En la actualidad, esta conducta se considera como una cuestión relacionada con las marcas comerciales. Como las violaciones a las marcas comerciales no están regidas por el presente Convenio, los encargados de su redacción consideraron apropiado abordar la cuestión del carácter delictivo de dicha conducta.

Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

43. Los delitos penales definidos más abajo en los Artículos 2 a 6 están destinados a proteger la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos y no asignan el carácter de delito a las actividades legítimas y comunes inherentes al diseño de las redes, o legítimas y comunes respecto de las prácticas comerciales y de operación.

Acceso ilícito (Artículo 2)

44. El término "acceso ilícito" abarca el delito básico que constituyen las amenazas peligrosas y los ataques a la seguridad (es decir, contra la confidencialidad, la integridad y la disponibilidad) de los sistemas y datos informáticos. La necesidad de protección refleja los intereses de las organizaciones y las personas para manejar, operar y controlar sus sistemas sin interrupciones ni restricciones. La mera intromisión no autorizada, es decir, la "piratería" (*hacking*), el "sabotaje" (*cracking*) o "la intrusión en el ordenador" (*computer trespass*) debería en principio ser ilícita en sí misma. Puede constituir un impedimento para los usuarios legítimos de los datos y sistemas y puede causar alteración o destrucción, lo que implica altos costos de reconstrucción. Dichas intromisiones pueden brindar acceso a datos confidenciales (incluidas las contraseñas y la información relacionada con los

sistemas a los que se pretende acceder) y a secretos con respecto al uso del sistema sin efectuar pago o incluso alentar a los piratas informáticos (*hackers*) a cometer formas más peligrosas de delitos informáticos, tales como los delito de fraude o falsificación informáticos.

45. El medio más eficaz de prevenir el acceso no autorizado es, por supuesto, la adopción y el desarrollo de medidas de seguridad eficaces. Sin embargo, una respuesta de amplio alcance debe incluir también la amenaza y el uso de medidas de derecho procesal. La prohibición penal en cuanto al acceso no autorizado puede brindar una protección adicional al sistema y a los datos propiamente dichos y en una primera etapa contra los peligros descritos más arriba.

46. El término "acceso" abarca la entrada a un sistema informático o a alguna parte del mismo (hardware, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados con los contenidos). Sin embargo, no incluye el mero envío de un mensaje de correo electrónico o de un archivo a ese sistema. El término "acceso" incluye el ingreso a otro sistema informático, al que esté conectado a través de redes de telecomunicaciones públicas, o a un sistema informático que esté conectado a la misma red, como una LAN (red de área local) o una Intranet (red interna) que opere en el seno de una organización. No tiene importancia el método de comunicación utilizado (por ej., desde lejos, incluidos los enlaces inalámbricos, o desde una corta distancia).

47. El acto debe también ser cometido de manera "ilegítima”. Además de la explicación dada más arriba, este término implica que el acceso autorizado por el propietario o por otro tenedor legítimo del sistema o de parte del mismo no constituye delito (como, por ej., a los fines de efectuar una verificación autorizada o de proteger el sistema informático en cuestión). Por otra parte, no constituye delito el acceder a un sistema informático que permite el acceso libre y abierto del público, ya que tal acceso es "legítimo".

48. La aplicación de instrumentos técnicos específicos puede dar lugar a un acceso conforme al Artículo 2, tal como el acceso a una página web, de manera directa o a través de enlaces de hipertexto, incluidos enlaces ocultos o la aplicación de "*cookies*" o "robots" para ubicar y recuperar información en aras de la comunicación. La aplicación de tales instrumentos no es *per se* "ilegítima”. El mantenimiento de un sitio web público implica el consentimiento por parte del propietario del sitio web que cualquier otro usuario de la red podrá acceder al mismo. La aplicación de las herramientas estándar provistas en los protocolos y programas de comunicación que comúnmente se aplican no es en sí misma "ilegítima”, en particular cuando se puede considerar que el tenedor legítimo del sistema al que se accede ha aceptado su aplicación, por ej., en el caso de las '*cookies*' al no rechazar la instalación inicial o por no eliminarla.

49. Muchas legislaciones nacionales ya contienen disposiciones referentes a los delitos de "piratería" (*hacking*), pero el alcance y los elementos constitutivos varían considerablemente. El enfoque amplio respecto de lo que constituye un delito contenido en la primera frase del Artículo 2 no es algo incontestado. Las controversias provienen de situaciones donde la mera intrusión no crea un peligro o cuando incluso los actos de piratería han dado lugar a la detección de "agujeros" y puntos débiles de los sistemas de seguridad. Esto ha llevado en una serie de países a la existencia de un enfoque más restringido que requiere circunstancias adicionales que añaden una matización, que es también el enfoque adoptado por la Recomendación núm. (89) 9 y la propuesta del Grupo de Trabajo de la OCDE en 1985.

50. Las Partes pueden adoptar el enfoque amplio y tipificar como delito a la piratería, de conformidad con la primera frase del Artículo 2. Alternativamente, las Partes pueden agregar algunos, o todos, las matizaciones que se enumeran en la segunda frase: infracción de las medidas de seguridad; intención especial de obtener datos informáticos; otras intenciones dolosas que justifiquen la responsabilidad penal, o la exigencia de que el delito se haya cometido en relación con un sistema informático que esté conectado de forma remota a otro sistema informático. La última opción permite que las Partes excluyan la situación en que una persona accede físicamente a un ordenador independiente sin valerse de otro sistema informático. Se puede restringir el delito de acceso ilícito a sistemas informáticos que estén conectados en red (incluidas las redes públicas provistas por los servicios de telecomunicaciones y las redes privadas, tales como intranets o extranets).

Interceptación ilícita (Artículo 3)

51. Esta disposición tiene como finalidad proteger el derecho a la privacidad de las comunicaciones de datos. El delito representa una violación de la privacidad de las comunicaciones tradicionales idéntica a la tradicional intervención y grabación de las conversaciones telefónicas orales entre las personas. El derecho a la privacidad de la correspondencia está consagrado en el Artículo 8 de la Convención Europea de Derechos Humanos. El delito establecido conforme al Artículo 3 aplica ese principio a todas las formas de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos.

52. El texto de la disposición ha sido extraído principalmente del delito de "intercepción no autorizada" contenida en la Recomendación (89) 9. En el presente Convenio se deja claro que las comunicaciones involucradas están relacionadas con las "transmisiones de datos informáticos", así como con las radiaciones electromagnéticas, en las circunstancias que se explican a continuación.

53. La interceptación por “medios técnicos” se refiere a escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos, ya sea en forma directa, mediante el acceso y uso del sistema informático, o en forma indirecta, mediante el uso de dispositivos electrónicos para escuchar en forma secreta o de dispositivos para intervenir conversaciones. La interceptación puede implicar también la grabación. El término “medios técnicos” incluye los dispositivos técnicos conectados a las líneas de transmisión, así como también los dispositivos utilizados para obtener y grabar las comunicaciones inalámbricas. Pueden incluir el uso de software, contraseñas y códigos. El requisito de que se utilice un medio técnico es una matización restrictiva destinada a evitar que se establezcan demasiados delitos.

54. El delito se aplica a las transmisiones "no públicas" de datos informáticos. El término "no públicas" matiza la naturaleza del proceso de transmisión (comunicación) y no la naturaleza de los datos transmitidos. Los datos comunicados pueden ser información que esté accesible al público, pero que las partes quieren comunicar de forma confidencial. También puede ocurrir que se desee mantener los datos en secreto con fines comerciales hasta que se pague por el servicio, como es el caso de la televisión de previo pago. Por lo tanto, el término "no pública" no excluye *per se* las comunicaciones que se realizan a través de las redes públicas. Las comunicaciones efectuadas por los empleados, ya sean o no con fines comerciales, que constituyen "transmisiones no públicas de datos informáticos" también están protegidas contra la interceptación sin permiso, en virtud del Artículo 3 (véase, por ej., la Sentencia de la Corte Europea de Derechos Humanos en el caso Halford contra el Reino Unido, del 25 de junio de 1997, 20.605/92).

55. La comunicación en la forma de transmisión de datos informáticos puede tener lugar dentro de un único sistema informático (por ej., pasando del CPU a la pantalla o la impresora), entre dos sistemas informáticos que pertenecen a una misma persona, entre dos ordenadores que se comunican entre sí, o entre un ordenador y una persona (por ej., a través del teclado). No obstante, las Partes podrán exigir como elemento adicional que la comunicación sea transmitida entre sistemas informáticos que estén conectados de forma remota.

56. Cabe señalar que el hecho de que la noción de "sistema informático" pueda incluir también las conexiones radioeléctricas no significa que una Parte tiene la obligación de establecer como delito la interceptación de cualquier transmisión de radio que, a pesar de ser "no pública", tenga lugar de manera relativamente abierta y sea fácil de acceder y en consecuencia pueda ser interceptada, por ejemplo, por los radioaficionados.

57. La creación de un delito en relación con “las emisiones electromagnéticas” asegurará un alcance más amplio. Las emisiones electromagnéticas pueden ser emitidas por un ordenador durante su funcionamiento. Dichas emisiones no son consideradas como 'datos' de

acuerdo con la definición establecida en el Artículo 1. Sin embargo, los datos pueden ser reconstruidos a partir de dichas emisiones. En consecuencia, la interceptación de los datos provenientes de las emisiones electromagnéticas de un sistema informático está incluida como un delito en virtud de este artículo.

58. Para que corresponda aplicar la responsabilidad penal, la interceptación ilegal debe ser cometida de manera "deliberada" e "ilegítima". El acto está justificado, por ejemplo, si la persona que intercepta la comunicación tiene permiso para hacerlo, si actúa bajo las órdenes o con la autorización de los participantes en la transmisión (incluidas la verificación autorizada o la protección de las actividades acordadas por los participantes), o si la vigilancia está legítimamente autorizada en el interés de la seguridad nacional o la detección de delitos por parte de las autoridades que los investigan. También está sobreentendido que no se pretende que el uso de prácticas comerciales comunes, tales como el empleo de '*cookies*', constituya un delito como tal, ya que no es una interceptación "ilegítima". Con respecto a las comunicaciones no públicas efectuadas por los empleados protegidos en virtud del Artículo 3 (véase el párrafo 54), las leyes nacionales pueden establecer las bases para la interceptación legítima de dichas comunicaciones. Conforme al Artículo 3, en tales circunstancias se consideraría que la interceptación es "legítima".

59. En algunos países, la interceptación puede estar estrechamente relacionada con el delito de acceso no autorizado a un sistema informático. Con el fin de garantizar la coherencia respecto de la prohibición y la aplicación de la ley, los países que requieren que exista una intención dolosa, o que el delito sea cometido en relación con un sistema informático que esté conectado a otro sistema informático, de conformidad con el Artículo 2, pueden requerir también matizaciones similares para aplicar la responsabilidad penal conforme a este artículo. Estos elementos deben ser interpretados y aplicados conjuntamente con los demás elementos del delito, como el hecho de ser "deliberada" e "ilegítima".

Ataques a la integridad de los datos (Artículo 4)

60. La finalidad de esta disposición es proporcionar a los datos informáticos y a los programas informáticos una protección similar a la que gozan los objetos corpóreos contra la imposición de un daño deliberado. El interés legal protegido en este caso es la integridad y el correcto funcionamiento o utilización de los datos almacenados o de los programas informáticos.

61. En el párrafo 1, los términos que "dañe" y "deteriore" como actos imbricados se refieren en particular a una alteración negativa de la integridad o del contenido de la información de los datos y programas. El "borrar" datos es el equivalente de la destrucción de un objeto corpóreo. Los destruye y los hace irreconocibles. Por "supresión" de datos informáticos se entiende

cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al ordenador o al soporte de datos en que fueron almacenados. El término “alteración" se refiere a la modificación de los datos existentes. Por consiguiente, la introducción de códigos maliciosos, tales como virus y caballos de Troya, está incluido en este párrafo, tal como también lo está la modificación resultante de los datos.

62. Los actos antes mencionados son punibles sólo si se cometen de manera "ilegítima”. Las actividades comunes inherentes al diseño de las redes o las prácticas comerciales o de operación comunes como, por ej., la verificación o la protección de la seguridad de un sistema informático autorizadas por el dueño o el operador, o la reconfiguración del sistema operativo de un ordenador que tenga lugar cuando el operador de un sistema adquiere un nuevo software (por ej., el software que permite el acceso a Internet que desactiva programas similares instalados previamente), son efectuadas de manera legítima y, en consecuencia, no constituyen un delito conforme a este artículo. La modificación de los datos relativos al tráfico con el fin de facilitar comunicaciones anónimas (por ejemplo, las actividades de los sistemas de redireccionamiento de mensajes de correo electrónico anónimos), o la modificación de datos con el fin de garantizar la seguridad de las comunicaciones (por ej., el cifrado) deberían en principio ser consideradas una forma de protección legítima de la vida privada y, por lo tanto, ser consideradas actividades legítimas. Sin embargo, las Partes tal vez deseen establecer como delito ciertos abusos relacionados con las comunicaciones anónimas, por ejemplo, cuando la información contenida en el encabezamiento del paquete es alterada con el fin de ocultar la identidad del autor del delito.

63. Además, el infractor debe haber actuado de manera “deliberada".

64. El párrafo 2 permite a las Partes formular una reserva concerniente a un delito en la que pueden exigir que la conducta tenga como resultado un perjuicio grave. La interpretación de lo que constituye dicho perjuicio grave queda a criterio de la legislación de cada país; con todo, las Partes deberían notificar su interpretación al Secretario General del Consejo de Europa si hacen uso de esta posibilidad de reserva.

Ataques a la integridad del sistema (Artículo 5)

65. La Recomendación núm. (89) 9 considera estos ataques como sabotaje informático. La disposición pretende establecer como delito el obstaculizar de manera deliberada el uso legítimo de los sistemas informáticos incluidos los servicios de telecomunicaciones utilizando o influenciando los datos informáticos. El interés jurídico protegido es el interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto. El texto está redactado en lenguaje neutral de manera tal que se pueda brindar protección a todo tipo de funciones.

66. El término "obstaculización" se refiere a las acciones que interfieren con el correcto funcionamiento del sistema informático. Dicha obstaculización debe efectuarse mediante la introducción, la transmisión, el daño, el borrado, la alteración o la supresión de datos informáticos.

67. La obstaculización debe además ser "grave", a fin de dar lugar a sanción penal. Cada Parte deberá determinar para sí los criterios que deberán cumplirse para que la obstaculización sea considerada "grave". Por ejemplo, una Parte puede exigir que se haya causado un mínimo de daños para que la obstaculización sea considerada grave. Los encargados de redactar el presente Convenio consideraron como "grave" el envío de datos a un sistema en particular cuando su forma, tamaño o frecuencia produzca un efecto perjudicial significativo en la capacidad que tiene el dueño o el operador para utilizar dicho sistema, o para comunicarse con otros sistemas (por ej., por medio de programas que generen ataques de "denegación del servicio", códigos maliciosos como los virus que impiden o hacen considerablemente más lento el funcionamiento del sistema, o programas que envían enormes cantidades de correo electrónico a un destinatario con el fin de bloquear las funciones de comunicación del sistema).

68. La obstaculización debe ser "ilegítima". Las actividades comunes inherentes al diseño de las redes, o las prácticas comerciales y de operación comunes, se efectúan de manera legítima. Las mismas incluyen, por ej., la verificación de la seguridad de un sistema informático, o su protección, autorizada por su propietario o por el operador, o la reconfiguración del sistema operativo de un ordenador que tiene lugar cuando el operador de un sistema instala un nuevo software que inhabilita programas similares previamente instalados. Por lo tanto, dicha conducta no constituye un delito conforme a este artículo, incluso si causa una obstaculización seria.

69. El envío de mensajes de correo electrónico no solicitados, con fines comerciales o de otra índole, puede causar un perjuicio a su receptor, en particular cuando dichos mensajes son enviados en grandes cantidades o con una elevada frecuencia (“bombardeo publicitario” o "*spamming*"). En opinión de quienes redactaron este Convenio, tal conducta debería constituir delito únicamente cuando sea deliberada y produzca una obstaculización grave de las comunicaciones. Sin embargo, las Partes pueden tener un enfoque diferente en cuanto a la obstaculización de las comunicaciones en su derecho interno, por ej., al establecer que ciertos actos de interferencia constituyen delitos administrativos o están sujetos a algún otro tipo de sanciones. El texto deja a criterio de las Partes la determinación del grado de obstaculización del funcionamiento del sistema –parcial o total, temporal o permanente – que se considera daño grave que justifique una sanción administrativa o penal, conforme a su derecho interno.

70. El delito debe ser cometido de manera deliberada; ello quiere decir que quien lo comete debe tener la intención de causar una obstaculización grave.

Abuso de los dispositivos (Artículo 6)

71. Esta disposición establece como delito separado e independiente la comisión deliberada de actos ilícitos específicos con respecto a ciertos dispositivos o datos de acceso que e utilizan mal con el fin de cometer los delitos antes descritos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos. Como la comisión de estos delitos a menudo requiere la posesión de medios de acceso ("herramientas de piratería") o de otras herramientas, existe un fuerte incentivo para adquirirlas con fines delictivos, lo que puede luego llevar a la creación de una especie de mercado negro para su producción y distribución. Con el fin de combatir dichos peligros con mayor eficacia, el derecho penal debería prohibir en su origen los actos específicos que sean potencialmente peligrosos, antes de que se cometan los delitos previstos en los Artículos 2 a 5. En lo que a esto se refiere, esta disposición se basa en desarrollos recientes en el seno del Consejo de Europa (Convenio Europeo sobre la protección jurídica de los servicios de acceso condicional o basados en dicho acceso – STE núm. 178) y de la Unión Europea (Directiva 98/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso) y las disposiciones pertinentes en algunos países. Un enfoque similar había sido ya adoptado en el Convenio internacional sobre represión de la falsificación de moneda firmado en Ginebra e 1929.

72. El párrafo 1.a).1 establece como delitos la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los Artículos 2 a 5 del presente Convenio. "Distribución" se refiere al acto de enviar datos a terceros, mientras que "la puesta a disposición" se refiere al poner en línea dispositivos para ser utilizados por otras personas. Este término se propone también abarcar la creación o compilación de hipervínculos con el fin de facilitar el acceso a dichos dispositivos. El término "programa informático" incluido en este Artículo se refiere a los programas concebidos, por ej., para alterar o incluso destruir datos o interferir con el funcionamiento de los sistemas, como es el caso de los virus, o programas concebidos o adaptados para lograr acceso a los sistemas informáticos.

73. Quienes redactaron el presente Convenio debatieron largamente si el término "dispositivos" debería restringirse a aquellos diseñados exclusivamente o específicamente para cometer delitos, excluyendo en consecuencia los dispositivos que tienen un uso dual. Se consideró que este criterio era demasiado limitado. Podría dar lugar a dificultades insuperables en relación con las pruebas necesarias en un procedimiento penal, por lo que la disposición podría resultar prácticamente inaplicable o aplicable sólo en contadas circunstancias. También se rechazó la alternativa de incluir todos

los dispositivos, incluso si son producidos y distribuidos de manera legal. En ese caso, únicamente el elemento subjetivo de la intención de cometer un delito informático sería decisivo para imponer un castigo, un enfoque que tampoco ha sido adoptado en el ámbito de la falsificación de monedas. Como un compromiso razonable el Convenio restringe su alcance a los casos en los que los dispositivos son objetivamente concebidos, o adaptados, principalmente con el fin de cometer un delito. Esto excluirá por lo general a los dispositivos de uso dual.

74. El inciso ii) del párrafo 1.a) establece como delitos la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático.

75. El párrafo 1.b) establece como delito la posesión de los elementos descritos en los incisos i) o ii) del párrafo 1.a). Conforme a la última frase del párrafo 1.b), las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal. El número de elementos poseídos está directamente relacionado con la prueba de que existió una intención delictiva. Queda a criterio de cada Parte decidir el número de elementos necesarios para que se considere que existe responsabilidad penal.

76. El delito requiere que se cometa de manera “deliberada” e "ilegítima”. Con el fin de evitar el peligro de establecer demasiados delitos cuando se producen y se introducen en el mercado dispositivos para fines legítimos, por ej., para contrarrestar los ataques contra los sistemas informáticos, se han agregado nuevos elementos para restringir el delito. Además del requisito general de que exista intención deliberada, debe estar presente la intención específica (es decir, directa) de utilizar el dispositivo para cometer cualquiera de los delitos establecidos en los Artículos 2 a 5 del presente Convenio.

77. El párrafo 2 deja claro que esta disposición no abarca las herramientas creadas para la verificación o protección autorizadas de un sistema informático. Este concepto ya está comprendido en el término "ilegítimo”. Por ejemplo, los dispositivos para someter a prueba los sistemas ("dispositivos de craqueo”) y los dispositivos para verificar las redes diseñados por la industria para controlar la fiabilidad de sus productos de tecnología de la información o para evaluar la seguridad de los sistemas son producidos con fines legítimos, y serían considerados “legítimos”.

78. Debido a diferentes estimaciones respecto de la necesidad de aplicar el delito de "abuso de los dispositivos" a todos los diferentes tipos de delitos informáticos incluidos en los Artículos 2 a 5, el párrafo 3 permite, en base a una reserva (véase el Artículo 42), la posibilidad de restringir el delito en el derecho interno. Sin embargo, todas las Partes están obligadas a tipificar como delito al menos la venta, distribución o puesta a disposición de una

contraseña informática o un código de acceso, como lo estipula el inciso ii) del párrafo 1.a).

Título 2 - Delitos informáticos

79. Los Artículos 7 a 10 se refieren a los delitos comunes que se cometen frecuentemente mediante la utilización de un sistema informático. Estos delitos comunes ya han sido tipificados como delitos por la mayoría de los Estados, cuyas leyes existentes pueden o no ser lo suficientemente amplias como para abarcar situaciones relacionadas con las redes informáticas (por ejemplo, las leyes existentes sobre pornografía infantil de algunos Estados pueden no abarcar las imágenes electrónicas). Por lo tanto, a la hora de aplicar estos artículos, los Estados deben examinar sus leyes vigentes para determinar si se aplican a situaciones en que estén involucradas redes y sistemas informáticos. Si los delitos existentes ya abarcan dicha conducta, no existe ninguna obligación de introducir enmiendas a los delitos existentes o de establecer nuevos delitos.

80. Las expresiones "falsificación informática" y "fraude informático" se refieren a determinados delitos relacionados con la informática; es decir, la falsificación informática y el fraude informático son dos tipos específicos de manipulación de los sistemas y los datos informáticos. Su inclusión reconoce el hecho de que en muchos países ciertos intereses legales tradicionales no están lo suficientemente protegidos contra las nuevas formas de interferencias y ataques.

Falsificación informática (Artículo 7)

81. La finalidad de este artículo es establecer un delito paralelo al de falsificación de documentos tangibles. Su objetivo es colmar algunas lagunas en el derecho penal en relación con el delito de falsificación tradicional, que requiere la legibilidad visual de las afirmaciones o declaraciones contenidas en un documento y que no se aplica a los datos almacenados electrónicamente. Las manipulaciones de dichos datos con valor probatorio pueden tener las mismas consecuencias graves que los actos de falsificación tradicionales si un tercero se ve así engañado. La falsificación informática implica la creación o la alteración ilegítimas de los datos almacenados de manera tal que adquieran un valor probatorio diferente en el transcurso de transacciones legales, que se basan en la autenticidad de la información contenida en los datos, y es objeto de un engaño. El interés jurídico que se desea proteger es la seguridad y la fiabilidad de los datos electrónicos, que pueden tener consecuencias para las relaciones legales.

82. Cabe señalar que los conceptos de falsificación varían mucho en la legislación interna de los diferentes países. En algunos, el concepto se basa en la autenticidad respecto del autor del documento y en otros está basado

en la veracidad de la declaración contenida en el documento. A pesar de ello, se llegó al acuerdo de que el engaño respecto de la autenticidad se refiere, como mínimo, al autor de los datos, independientemente de la exactitud o la veracidad de los contenidos de los mismos. Las Partes pueden ampliar este concepto e incluir en el término "autenticidad" el carácter genuino de los datos.

83. Esta disposición abarca datos que sean equivalentes a un documento de carácter público o privado, que tenga efectos legales. La "introducción" no autorizada de datos correctos o incorrectos produce una situación que se corresponde con la elaboración de un documento falso. Las posteriores alteraciones (modificaciones, variaciones, cambios parciales), borrado (eliminación de datos de un soporte de datos) y supresiones (retención, ocultación de datos) corresponden en general al delito de falsificación de un documento auténtico.

84. La expresión "a efectos legales" se refiere también a las transacciones y documentos legales que son relevantes desde el punto de vista jurídico.

85. La última frase de la disposición permite a las Partes, al aplicar el delito con arreglo a su derecho interno, exigir además que debe existir la intención de engañar o una intención dolosa similar, para que se considere que existe responsabilidad penal.

Fraude informático (Artículo 8)

86. Con la llegada de la revolución tecnológica, se han multiplicado las oportunidades para cometer delitos económicos como el fraude, incluido el fraude de tarjetas de crédito. Los bienes representados o administrados a través de sistemas informáticos (fondos electrónicos, depósitos) se han convertido en el blanco de manipulaciones del mismo modo que las formas tradicionales de bienes. Estos delitos consisten principalmente en manipulaciones respecto de la introducción de datos, cuando se introducen datos incorrectos en un ordenador, o en manipulaciones respecto de los programas y otras interferencias al procesamiento de los datos. La finalidad de este artículo es establecer como delito toda manipulación indebida realizada en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes.

87. Para garantizar que están cubiertas todas las posibles manipulaciones relevantes, los elementos constitutivos de la "introducción", "alteración", "borrado" o "supresión" mencionados en el Artículo 8.a) se complementan por el acto general de "interferir con el funcionamiento de un programa o sistema informático" en el Artículo 8.b). Los elementos constituyentes de una "introducción", "alteración", "borrado" o "supresión" tienen un significado idéntico al establecido en los artículos anteriores. El Artículo 8.b) abarca actos tales como manipulaciones de los equipos, actos que impiden la

impresión y actos que impiden la grabación o el flujo de los datos, o la secuencia en que se ejecutan los programas.

88. Las manipulaciones relacionadas con el fraude informático constituyen un delito si causan a otra persona perjuicio patrimonial directo, pérdida de la posesión de un bien, y si el autor actuó de manera deliberada para obtener de manera ilegítima un beneficio económico para sí mismo o para otra persona. El término "perjuicio patrimonial", que es un concepto amplio, incluye la pérdida de dinero y de cosas tangibles e intangibles que tengan un valor económico.

89. El delito debe ser cometido de forma "ilegítima", y el beneficio económico debe obtenerse de manera ilegítima. Por supuesto, no se pretende incluir en el delito establecido en este artículo aquellas prácticas comerciales comunes legítimas, destinadas a obtener un beneficio económico, ya que las mismas se realizan legítimamente. Por ejemplo, son legítimas las actividades llevadas a cabo en virtud de un contrato válido entre las personas afectadas (por ej., inhabilitar un sitio web a realizar las funciones conferidas en los términos del contrato).

90. El delito debe ser cometido de manera "deliberada". El elemento general de la intención deliberada se refiere a la manipulación o la interferencia de los equipos informáticos que cause un perjuicio patrimonial a un tercero. El delito requiere también la existencia de una intención deliberada específica de índole fraudulenta o dolosa para obtener un beneficio económico o de otro tipo para sí o para otra persona. Así, por ejemplo, no se pretende incluir en el delito establecido por este artículo aquellas prácticas comerciales con respecto a la competencia en el mercado, que pueden causar un perjuicio patrimonial a una persona y beneficiar a otra, pero que no son llevadas a cabo con una intención fraudulenta o dolosa. Por ejemplo, no se pretende establecer como delito el uso de programas que reúnen información para comparar los precios de las compras que se pueden hacer por Internet ("bots"), incluso si no son autorizados por un sitio visitado por el "bot".

Título 3 - Delitos relacionados con el contenido

Delitos relacionados con la pornografía infantil (Artículo 9)

91. El Artículo 9 referente a la pornografía infantil tiene como finalidad reforzar las medidas de protección de los menores, incluida su protección contra la explotación sexual, mediante la modernización de las disposiciones del derecho penal con el fin de circunscribir de manera más eficaz la utilización de los sistemas informáticos en relación con la comisión de delitos de índole sexual contra menores.

92. Esta disposición responde a la preocupación de los Jefes de Estado y de Gobierno del Consejo de Europa, expresada en su 21a

Cumbre (Estrasburgo, 10 a 11 de octubre de 1997) en su Plan de Acción (punto III.4) y está acorde con la tendencia internacional encaminada a lograr la prohibición de la pornografía infantil, como se evidencia por la reciente adopción del Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía y por la reciente iniciativa de la Comisión Europea relativa a la lucha contra la explotación sexual de los niños y la pornografía (COM2000/854).

93. Esta disposición establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil. La mayoría de los Estados ya han establecido como delito la producción tradicional y la distribución física de pornografía infantil; con todo, debido al creciente uso de Internet como principal instrumento para el comercio de tales materiales, se consideró sin lugar a dudas que era esencial establecer disposiciones específicas en un instrumento jurídico internacional para combatir esta nueva forma de explotación sexual que representa un peligro para los menores. La opinión generalizada es que los materiales y prácticas en línea tales como el intercambio de ideas, fantasías y consejos entre los pedófilos, desempeñan un papel para apoyar, alentar o facilitar los delitos de índole sexual contra los menores.

94. El párrafo 1.a) establece como delito la producción de pornografía infantil con la intención de difundirla a través de un sistema informático. Esta disposición se consideró necesario para luchar contra los peligros descritos anteriormente con respecto a su origen.

95. El párrafo 1.b) establece como delito la "oferta" de pornografía infantil a través de un sistema informático. El término "oferta" se propone abarcar el hecho de pedir a otros que obtengan pornografía infantil. Implica que la persona que ofrece el material puede en realidad proporcionarlo. El término "puesta a disposición" se propone abarcar el hecho de poner en línea pornografía infantil para que sea utilizada por terceros, por ej., mediante la creación de sitios de pornografía infantil. Este párrafo se propone también abarcar la creación o la recopilación de hipervínculos a sitios de pornografía infantil con el fin de facilitar el acceso a dichos sitios.

96. El párrafo 1.c) establece como delito la difusión o la transmisión de pornografía infantil a través de un sistema informático. La "difusión" es la diseminación activa del material. El hecho de enviar pornografía infantil a otra persona a través de un sistema informático estaría comprendido dentro del delito de "transmisión" de pornografía infantil.

97. La expresión "la adquisición, para uno mismo o para otros" en el párrafo 1.d) significa obtener activamente pornografía infantil, por ej., descargándola.

98. La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos, como un disquete o CD-ROM, es considerada delito en el párrafo 1.e). La posesión de pornografía infantil estimula la demanda de dichos materiales. Una manera eficaz de reducir la producción de pornografía infantil es imponer consecuencias penales a la conducta de cada participante que interviene en la cadena desde la producción hasta la posesión.

99. El término "material pornográfico" en el párrafo 2 se rige por las normas nacionales relativas a la clasificación de los materiales como obscenos, incompatibles con la moral pública o similarmente corruptos. Por consiguiente, puede considerarse que los materiales que tienen un mérito artístico, médico, científico o similares características no son pornográficos. La representación visual incluye los datos almacenados en una disquete de o en otro medio electrónico de almacenamiento de datos informáticos que puedan convertirse en imágenes visuales.

100. La expresión "comportamiento sexualmente explícito" abarca por lo menos las siguientes alternativas, tanto en forma real como simulada: a) las relaciones sexuales, ya sea en forma genital-genital, oral-genital, anal-genital u oral-anal, entre menores, o entre un adulto y un menor, del mismo sexo o del sexo opuesto; b) la bestialidad; c) la masturbación; d) los abusos sádicos o masoquistas en un contexto sexual, o e) la exhibición lasciva de los genitales o la zona púbica de un menor. Es indiferente el hecho de que la conducta descrita sea real o simulada.

101. Los tres tipos de materiales definidos en el párrafo 2 a los fines de la comisión de los delitos mencionados en el párrafo 1 abarcan las representaciones de abuso sexual de un niño real (2.a), las imágenes pornográficas que muestran a una persona que parezca un menor adoptando un comportamiento sexualmente explícito (2b), y, finalmente, las imágenes que, si bien "realistas", no implican de hecho la participación de un niño real en un comportamiento sexualmente explícito (2.c). Este última posibilidad incluye las imágenes alteradas, tales como las imágenes modificadas de personas físicas, o incluso generadas totalmente por medios informáticos.

102. En los tres casos previstos en el párrafo 2, los intereses legales que se protegen son ligeramente diferentes. El párrafo 2.a) se centra más directamente en la protección contra el abuso de menores. Los párrafos 2.b) y 2.c) se proponen brindar protección contra comportamientos que, si bien no necesariamente causan daños al "menor" representado en el material, ya que podría no existir un menor real, podrían ser utilizados para alentar o seducir a niños para que participen en dichos actos y, en consecuencia, forman parte de una subcultura que favorece el maltrato de menores.

103. El término "ilegítimo" no excluye las defensas, excusas o principios legales pertinentes similares que eximen a una persona de responsabilidad en circunstancias específicas. Por consiguiente, el término "ilegítimo" permite

que una Parte tome en cuenta los derechos fundamentales, tales como la libertad de pensamiento, de expresión y de la vida privada. Por otra parte, una Parte puede establecer una defensa respecto de una conducta relacionada con un "material pornográfico" que tenga un mérito artístico, médico, científico o de similares características. En relación con el párrafo 2.b), la referencia al término "ilegítimo" podría también permitir, por ej., que una Parte pueda decidir que una persona queda eximida de responsabilidad penal si se demuestra que la persona representada no es un menor en el sentido de lo que aquí se dispone.

104. El párrafo 3 define el término "menor" en relación con la pornografía infantil en general, entendiendo como "menor" toda persona menor de 18 años, conforme con la definición de "menor" contenida en la Convención de las Naciones Unidas sobre los Derechos del Niño (Artículo 1). Se consideró que era una importante cuestión de política establecer una norma internacional uniforme con respecto a la edad. Cabe señalar que la edad se refiere al uso de menores (reales o ficticios) como objetos sexuales, y no a la edad necesaria para consentir una relación sexual.

Sin embargo, reconociendo que algunos Estados exigen un límite de edad inferior en su legislación nacional respecto de la pornografía infantil, la última frase del párrafo 3 prevé que las Partes podrán exigir un límite de edad diferente, siempre y cuando no sea inferior a 16 años.

105. Este artículo enumera diferentes tipos de actos ilícitos en relación con la pornografía infantil que, conforme a los Artículos 2 a 8, las Partes están obligadas a tipificar como delito si fueron cometidos de manera "deliberada". Conforme a este criterio, una persona no es responsable a menos que tenga la intención de ofrecer, poner a disposición, distribuir, transmitir, producir o poseer pornografía infantil. Las Partes pueden adoptar una norma más específica (véase, por ejemplo, la legislación aplicable en la Comunidad Europea en relación con la responsabilidad de los proveedores de servicios), en cuyo caso regirá dicha norma. Por ejemplo, la responsabilidad puede ser impuesta si existe un "conocimiento y control" de la información que es transmitida o almacenada. No es suficiente, por ejemplo, que un proveedor de servicios haya servido de conducto para el material, o albergado un sitio web o sala de noticias que contuviera dicho material, si no existió la intención exigida conforme al derecho interno respecto al caso particular. Por otra parte, un proveedor de servicios no está obligado a verificar conductas para evitar una responsabilidad penal.

106. El párrafo 4 permite a las Partes hacer reservas respecto de los apartados d) y e) del párrafo 1), y los apartados b) y c) del párrafo 2). El derecho a no aplicar esas partes de la disposición puede ejercerse en forma total o parcial. Toda reserva de esa índole debería ser notificada por las Partes al Secretario General del Consejo de Europa al momento de la firma o al depositar los instrumentos de ratificación, aceptación, aprobación o adhesión, de conformidad con el Artículo 42.

Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Artículo 10)

107. Las infracciones de los derechos de propiedad intelectual, en particular del derecho de autor, se cuentan entre los delitos más comunes cometidos por Internet, lo que causa preocupación tanto a los titulares de derechos de autor como a aquellos que trabajan profesionalmente con redes informáticas. La reproducción y difusión a través de Internet de obras que están protegidas, sin la autorización del titular del derecho de autor, son extremadamente frecuentes. Dichas obras protegidas incluyen las obras literarias, fotográficas, musicales, audiovisuales y demás. La facilidad con que se pueden hacer copias no autorizadas gracias a la tecnología digital y la escala de reproducción y de difusión en el contexto de las redes electrónicas hizo necesario incluir disposiciones referentes a las sanciones penales y aumentar la cooperación internacional en este campo.

108. Cada Parte tiene la obligación de tipificar como delito las infracciones deliberadas de los derechos de autor y otros derechos conexos, a veces denominados derechos afines, derivados de los acuerdos enumerados en el Artículo, "cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático". El párrafo 1 establece sanciones penales contra las infracciones de la propiedad intelectual por medio de un sistema informático. La violación de los derechos de autor ya es considerada un delito en la mayoría de los Estados. El párrafo 2 trata de la violación de los derechos afines por medio de un sistema informático.

109. Las infracciones de la propiedad intelectual y de los derechos afines conforme se definen con arreglo al derecho interno de cada Parte y de conformidad con las obligaciones que cada Parte haya contraído respecto de ciertos instrumentos internacionales. Si bien cada Parte tiene la obligación de tipificar como delito esas infracciones, la manera precisa en la cual tales infracciones se definen en la legislación nacional puede variar de un Estado a otro. Sin embargo, las obligaciones relativas a la tipificación como delito en virtud del Convenio cubren solo las infracciones de la propiedad intelectual abordadas de manera explícita en el Artículo 10 y, por lo tanto, excluyen las infracciones de patentes o de marcas comerciales.

110. Con respecto al párrafo 1, los acuerdos a que se hace referencia son el Convenio de Berna para la Protección de las Obras Literarias y Artísticas - Acta de París del 24 de julio de 1971; el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el comercio (ADPIC) y el Tratado de la OMPI sobre Derechos de Autor. Con respecto al párrafo 2, los instrumentos internacionales citados son: la Convención Internacional sobre

la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma, 1961), el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el comercio (ADPIC) y el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Interpretación o Ejecución y Fonogramas. El uso de la expresión "de conformidad con las obligaciones que haya contraído" en ambos párrafos deja en claro que las Partes Contratantes del presente Convenio no están obligadas a aplicar los acuerdos citados en los cuales no sean Parte; además, si una Parte ha formulado una reserva o declaración permitida en uno de los acuerdos, dicha reserva puede limitar el alcance de su obligación en virtud del presente Convenio.

111. El Tratado de la OMPI sobre Derechos de Autor y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas no habían entrado en vigor en la fecha de la celebración del presente Convenio. Sin embargo, esos tratados son importantes, ya que actualizan considerablemente la protección de la propiedad intelectual a nivel internacional (especialmente en lo que respecta al nuevo derecho de "poner a disposición" material protegido "bajo demanda" a través de Internet) y mejoran los medios para combatir las violaciones de los derechos de propiedad intelectual en todo el mundo. Sin embargo, se entiende que las infracciones de los derechos establecidos en esos tratados no deben ser tipificados como delito por el presente Convenio hasta que esos tratados hayan entrado en vigor con respecto a una Parte.

112. La obligación de tipificar como delito las infracciones de la propiedad intelectual y de los derechos afines en virtud de las obligaciones contraídas en los instrumentos internacionales no es extensiva a los derechos morales conferidos por los citados instrumentos (como en el Artículo 6 bis del Convenio de Berna y en el Artículo 5 del Tratado de la OMPI sobre Derechos de Autor).

113. Los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines deben ser cometidos "deliberadamente" para que corresponda aplicar la responsabilidad penal. En contraste con todas las demás disposiciones de derecho sustantivo de este Convenio, en los párrafos 1 y 2 se utiliza el término "deliberadamente" en lugar de manera "deliberada", ya que éste es el término empleado en el Acuerdo sobre los ADPIC (Artículo 61), que rige la obligación de establecer como delito las violaciones de los derechos de autor.

114. Las disposiciones están destinadas a establecer sanciones penales contra las infracciones "a escala comercial" y por medio de un sistema informático. Esto está en consonancia con el Artículo 61 del Acuerdo sobre los ADPIC, que requiere la aplicación de sanciones penales en las cuestiones relacionadas con la propiedad intelectual sólo en el caso de la "piratería a escala comercial". Sin embargo, las Partes tal vez deseen no limitarse a las

actividades "a escala comercial" y tipificar como delitos también otros tipos de infracciones de la propiedad intelectual.

115. El término "ilegítimo" se ha omitido del texto de este artículo por ser redundante, ya que el término "infracción" denota ya el uso de manera "ilegítima" del material sujeto a los derechos de autor. La ausencia del término "ilegítimo" no excluye *a contrario* la aplicación de las defensas, justificaciones y principios del derecho penal que rigen respecto de la exención de la responsabilidad penal asociada con el término "ilegítimo" en cualquier otro punto del Convenio.

116. El párrafo 3 permite a las Partes reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 en "circunstancias bien delimitadas" (por ejemplo, las importaciones paralelas, los derechos de alquiler), siempre y cuando se disponga de otros recursos eficaces, incluidos los derechos civiles y/o las medidas administrativas. Esta disposición en esencia otorga a las Partes una exención limitada respecto de la obligación de imponer una responsabilidad penal, siempre y cuando no dejen sin efecto las obligaciones contraídas en virtud del Artículo 61 del Acuerdo sobre los ADPIC, que es el requisito mínimo existente respecto de la penalización.

117. Este artículo no puede interpretarse en modo alguno como que extiende la protección otorgada a los autores, productores cinematográficos, intérpretes o ejecutantes, productores de fonogramas, entidades de radiodifusión o a otros titulares de derechos a aquellas personas que no reúnen las condiciones necesarias para estar incluidas en este grupo conforme a la legislación nacional o los acuerdos internacionales.

Título 5 – Otras formas de responsabilidad y de sanción

Tentativa y complicidad (Artículo 11)

118. La finalidad de este artículo es establecer otros delitos relacionados con la tentativa y la complicidad o la instigación de los delitos contemplados en el Convenio. Como se analiza más adelante, no es necesario que una Parte tipifique como delito la tentativa de cometer cada uno de los delitos establecidos en el Convenio.

119. El párrafo 1 exige que las Partes establezcan como delitos penales el acto de ayudar o instigar a la comisión de cualquiera de los delitos previstos en aplicación de los Artículos 2 al 10. Se incurrirá en responsabilidad por brindar ayuda o por complicidad cuando la persona que comete un delito establecido en el Convenio recibe ayuda de otra persona que también tiene la intención de cometer el delito. Por ejemplo, si bien la transmisión de datos relativos a contenidos perjudiciales o a códigos maliciosos a través de Internet requiere la ayuda de los proveedores de servicios como canal de transmisión, no puede recaer responsabilidad en un proveedor de servicios

que no tiene la intención de delinquir en virtud de lo dispuesto en esta sección. Así, el proveedor de servicios no está en la obligación de verificar activamente los contenidos para evitar una responsabilidad penal conforme a esta disposición.

120. En cuanto al párrafo 2, relativo a la tentativa, se estimó que algunos de los delitos definidos en el Convenio, o elementos de esos delitos, presentaban dificultades conceptuales (por ejemplo, los elementos consistentes en ofrecer o poner a disposición pornografía infantil). Por otra parte, algunos sistemas jurídicos limitan los delitos en los que la tentativa es sancionada. En consecuencia, sólo se requiere que la tentativa sea tipificada como delito en relación con los delitos establecidos en aplicación de los Artículos 3, 4, 5, 7, 8, 9 1).a) y 9 1).c).

121. Como ocurre con todos los delitos establecidos conforme al Convenio, el delito de tentativa y complicidad o instigación deberá ser cometido de manera deliberada.

122. El párrafo 3 se ha añadido para dar cuenta de las dificultades que puedan tener las Partes respecto de la aplicación del párrafo 2, en vista de la amplia variedad de conceptos contenidos en el derecho interno de los distintos países, a pesar del esfuerzo realizado en el párrafo 2 para eximir ciertos aspectos de la disposición relativa a la tentativa. Una Parte puede declarar que se reserva el derecho de no aplicar el párrafo 2, en todo o en parte. Esto significa que cualquiera de las Partes que formule una reserva con respecto a esa disposición no estará obligada a tipificar como delito la tentativa, o puede elegir los delitos o las partes de los delitos a los cuales se aplicarán las sanciones penales en relación con la tentativa. La reserva tiene por objeto posibilitar la más amplia ratificación del Convenio, mientras que al mismo tiempo autoriza a las Partes a preservar algunos de sus conceptos jurídicos fundamentales.

Responsabilidad de las personas jurídicas (Artículo 12)

123. El artículo 12 versa sobre la responsabilidad de las personas jurídicas. Es coherente con la tendencia jurídica actual de reconocer la responsabilidad de las personas jurídicas. Tiene como finalidad imponer la responsabilidad a las empresas, asociaciones y personas jurídicas de similares características por las acciones penales llevadas a cabo por una persona que ejerza funciones directivas en su seno, cuando dichas acciones sean llevadas a cabo para beneficio de la persona jurídica. El Artículo 12 también contempla la posibilidad de exigir responsabilidad cuando una persona que ejerza funciones directivas no vigile o controle debidamente a un empleado o representante de la persona jurídica, en caso de que dicha ausencia de vigilancia o de control facilite la comisión por parte de ese empleado o agente de uno de los delitos previstos en aplicación de este Convenio.

124. En virtud del párrafo 1, es necesario que se cumplan cuatro condiciones para que pueda exigirse responsabilidad. En primer lugar, debe haberse cometido uno de los delitos previstos en el presente Convenio. En segundo lugar, el delito debe haber sido cometido en beneficio de la persona jurídica. En tercer lugar, una persona que ejerza funciones directivas debe haber cometido el delito (incluida la complicidad y la instigación). Por "persona que ejerza funciones directivas" se entiende una persona física que tiene un alto cargo en la organización, como un director. En cuarto lugar, la persona que ejerce funciones directivas debe haber actuado basándose en una de las siguientes facultades: un poder de representación de la persona jurídica, una autorización para tomar decisiones en nombre de la persona jurídica, o una autorización para ejercer funciones de control en el seno de la persona jurídica, lo que demuestra que dicha persona física actuó conforme a sus facultades para comprometer la responsabilidad de la persona jurídica. En síntesis, el párrafo 1 obliga a las Partes a tener la capacidad de exigir responsabilidad a una persona jurídica sólo en el caso de los delitos cometidos por las personas que ejerzan funciones directivas.

125. Además, el párrafo 2 obliga a las Partes a tener la capacidad de exigir responsabilidades a una persona jurídica cuando el delito es cometido no por la persona que ejerza funciones directivas descritas en el párrafo 1, sino por otra persona que actúe bajo la autoridad de la persona jurídica, es decir, uno de sus empleados o agentes que actúe en el ámbito de su autoridad. Las condiciones que deben cumplirse antes de que la responsabilidad recaiga sobre la persona jurídica son que: 1) dicho empleado o agente de la persona jurídica debe haber cometido un delito; 2) el delito se ha cometido en beneficio de la persona jurídica, y 3) la comisión del delito ha sido posible porque la persona que ejercía funciones directivas no vigiló o controló al empleado o agente. En este contexto, debe interpretarse que la falta de vigilancia o de control incluye el no tomar las medidas apropiadas y razonables para impedir que los empleados o agentes cometan actividades delictivas en nombre de la persona jurídica. Dichas medidas apropiadas y razonables podrían ser determinadas por varios factores, tales como el tipo de empresa, su tamaño, las normas o las prácticas óptimas establecidas en ese tipo de negocio, etc. Esto no debería interpretarse como que se exige un régimen de vigilancia general sobre las comunicaciones de los empleados (véase también el párrafo 54). Un proveedor de servicios no incurre en ninguna responsabilidad por el hecho de que el delito se hubiere cometido en su sistema por parte de un cliente, usuario u otra persona, ya que el término "actúe bajo su autoridad" se aplica exclusivamente a los empleados y agentes que actúan en el ámbito de su autoridad.

126. La responsabilidad en virtud del presente artículo puede ser penal, civil o administrativa. Cada Parte tiene la flexibilidad de elegir establecer alguna o todas esas formas de responsabilidad, con arreglo a los principios jurídicos de cada Parte, siempre y cuando cumpla con los criterios del Artículo 13, párrafo 2, en que se establece que las sanciones o medidas deben ser "efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias”.

127. El párrafo 4 aclara que la responsabilidad de las personas jurídicas no excluye la responsabilidad individual de las personas físicas.

Sanciones y medidas (Artículo 13)

128. Este Artículo está estrechamente relacionado con los Artículos 2 a 11, que definen diversos delitos informáticos o delitos relacionados con la informática que deberían estar sujetos a sanciones conforme al derecho penal. De conformidad con las obligaciones impuestas por dichos artículos, esta disposición obliga a las Partes Contratantes a sacar consecuencias de la grave naturaleza de estos delitos al establecer la imposición de sanciones penales "efectivas, proporcionadas y disuasorias" y, en el caso de las personas físicas, la posibilidad de imponer penas de privación de libertad.

129. Las personas jurídicas a las que se exigirá responsabilidad de conformidad con lo dispuesto en el Artículo 12 deberán también estar sujetas a sanciones "efectivas, proporcionadas y disuasorias", que pueden ser de naturaleza penal, civil o administrativa. En virtud del párrafo 2, las Partes Contratantes están obligadas a prever la posibilidad de imponer sanciones pecuniarias a las personas jurídicas.

130. Este Artículo deja abierta la posibilidad de imponer otras sanciones y medidas que reflejen la gravedad de los delitos; por ejemplo, las medidas podrían incluir un mandamiento judicial o una orden de confiscación. Deja a criterio de las Partes la facultad discrecional para crear un sistema de delitos penales y de sanciones que sea compatible con sus respectivos sistemas jurídicos existentes.

Sección 2 - Derecho procesal

131. Los artículos de esta Sección describen algunas medidas procesales que deben adoptarse a nivel nacional con el fin de facilitar la investigación penal de los delitos establecidos en la Sección 1, otros delitos cometidos por medio de un sistema informático y la obtención de pruebas en formato electrónico relativas a un delito penal. De conformidad con el Artículo 39, párrafo 3, nada en el Convenio requiere o invita a una Parte a establecer facultades o procedimientos distintos a los que figuran en el presente Convenio, ni impide que una Parte los establezca.

132. La revolución tecnológica, que incluye la "autopista electrónica", en que numerosas formas de comunicación y servicios están interrelacionadas e interconectadas y comparten medios de transmisión y transporte convencionales, ha alterado la esfera del derecho penal y los procedimientos penales. La constante expansión de la red de comunicaciones abre nuevas puertas para la actividad delictiva por lo que respecta tanto a los delitos

tradicionales como a los nuevos delitos tecnológicos. El derecho penal sustantivo no es el único que debe mantenerse al tanto de estos nuevos abusos, ya que también es necesario que lo estén el derecho procesal penal y las técnicas de investigación. Del mismo modo, se deben adaptar o desarrollar salvaguardias para mantenerse al corriente del nuevo entorno tecnológico y de las nuevas facultades procesales.

133. Uno de los principales desafíos que se plantean en la lucha contra los delitos que se cometen en el entorno de las redes interconectadas es la dificultad para identificar al autor del delito y para estimar la magnitud y el impacto del acto delictivo. Otro problema obedece a la volatilidad de los datos electrónicos, que pueden ser alterados, movidos o borrados en cuestión de segundos. Por ejemplo, un usuario que tiene el control de los datos puede utilizar el sistema informático para borrar datos que son objeto de una investigación penal, destruyendo así las pruebas. La velocidad y, a veces, el secreto son a menudo vitales para el éxito de una investigación.

134. El presente Convenio adapta las medidas procesales tradicionales, tales como el registro y confiscación, al nuevo entorno tecnológico. Además, se han creado nuevas medidas, tales como la conservación rápida de los datos, con el fin de garantizar que las medidas tradicionales para obtener información, tales como el registro y la confiscación, seguirán siendo eficaces en el volátil entorno tecnológico. Como los datos en el nuevo entorno tecnológico no siempre son estáticos, sino que pueden estar en movimiento en el proceso de comunicación, se han adaptado otros procedimientos tradicionales de obtención de información pertinentes para las telecomunicaciones, tales como la obtención en tiempo real de los datos relativos al tráfico y la interceptación de los datos relativos al contenido, con el fin de permitir la obtención de los datos electrónicos que se encuentran en el proceso de la comunicación. Algunas de estas medidas forman parte de la Recomendación núm. R (95) 13 del Consejo de Europa respecto de los problemas del derecho procesal penal en relación con la tecnología de la información.

135. Todas las disposiciones contempladas en la presente Sección tienen como finalidad permitir la obtención o la obtención de datos a los fines de llevar a cabo investigaciones o procedimientos penales específicos. Quienes redactaron el presente Convenio debatieron si éste debería imponer a los proveedores de servicios la obligación de obtener los datos relativos al tráfico y de conservarlos por un período de tiempo determinado, pero finalmente no se incluyó ninguna obligación de esa índole debido a la falta de consenso.

136. Los procedimientos en general se refieren a todo tipo de datos, incluidos tres tipos específicos de datos informáticos (datos relativos al tráfico, datos acerca de los contenidos y datos sobre los abonados), que pueden existir en dos formas (almacenados o en el proceso de la comunicación). En los Artículos 1 y 18 se presentan definiciones de algunos de estos términos. La aplicabilidad de un procedimiento a un determinado tipo o formato de datos

electrónicos depende de la naturaleza y del formato de los datos y de la índole del procedimiento, tal como se describe específicamente en cada artículo.

137. Al adaptar las leyes procesales tradicionales al nuevo entorno tecnológico se planteó el problema de elegir la terminología apropiada en las disposiciones de esta sección. Las opciones incluían mantener el lenguaje tradicional (“registro” y “confiscación”), usar términos informáticos nuevos y más orientados a la tecnología (“acceder” y “copiar”), como los adoptados en los textos de otros foros internacionales sobre el tema (como el subgrupo de Delitos de Alta Tecnología del Grupo de los 8), o emplear una combinación de términos (“registrar o acceder de manera similar”, y “confiscar o conseguir de manera similar"). En vista de la necesidad de reflejar la evolución de los conceptos en el entorno electrónico, y de identificar y mantener también sus raíces tradicionales, se adoptó un enfoque flexible consistente en permitir que los Estados empleen tanto las viejas nociones de "registro y confiscación" como las nuevas nociones de "acceso y copia".

138. Todos los artículos incluidos en esta Sección se he mención a las "autoridades competentes" y a las facultades que deben conferírseles a los fines de llevar a cabo investigaciones o procedimientos penales específicos. En algunos países, solo los jueces tienen la facultad de ordenar o autorizar la obtención o presentación de pruebas, mientras que en otros países los fiscales o los funcionarios encargados de aplicar las leyes tienen las mismas o similares facultades. Por lo tanto, por "autoridad competente" se entiende un cuerpo encargado del cumplimiento de la ley, ya sea judicial, administrativo o de otra índole, que esté facultado conforme a la legislación de cada país para ordenar, autorizar o llevar a cabo la ejecución de medidas procesales a los fines de obtener o presentar pruebas en relación con investigaciones o procedimientos penales específicos.

Título 1 - Disposiciones comunes

139. La sección comienza con dos disposiciones de carácter general que se aplican a todos los artículos relativos al derecho procesal.

Ámbito de aplicación de las disposiciones de procedimiento (Artículo 14)

140. Cada Estado que sea Parte en el presente Convenio está obligado a adoptar las medidas legislativas y de otra índole que resulten necesarias, de conformidad con su derecho interno y su marco jurídico, para establecer los poderes y procedimientos previstos en esta Sección a los efectos de la "investigación o de procedimientos penales específicos."

141. Sujeto a dos excepciones, cada Parte aplicará los poderes y procedimientos mencionados en esta Sección: i) a los delitos previstos en aplicación de la Sección 1 del presente Convenio; ii) a cualquier otro delito cometido por medio de un sistema informático; y iii) a la obtención de pruebas electrónicas de cualquier delito. Así, a los fines de llevar a cabo investigaciones y procedimientos penales específicos, los poderes y los procedimientos contemplados en esta Sección deberán ser aplicados a los delitos establecidos conforme al Convenio, a otros delitos cometidos mediante el uso de un sistema informático, y a la obtención de pruebas en formato electrónico de un delito penal. Esto asegura que se pueden obtener o recopilar pruebas en formato electrónico de cualquier delito con arreglo a los poderes y procedimientos establecidos en esta Sección. Esto asegura una capacidad para obtener o recopilar datos informáticos que es equivalente o paralela a la que existe en virtud de los poderes y procedimientos aplicables a los datos que no se encuentran en formato electrónico. El Convenio establece explícitamente que las Partes deberían incorporar en sus leyes la posibilidad de que la información contenida en formato digital, o en otro tipo de formato electrónico, pueda ser utilizada como prueba ante un tribunal en un juicio penal, independientemente de la índole del delito que se esté juzgando.

142. Existen dos excepciones respecto del ámbito de aplicación. En primer lugar, el Artículo 21 establece que la facultad de interceptar los datos relativos al contenido deberá estar limitada a una serie de delitos graves que serán determinados por la legislación nacional. Muchos estados limitan el poder de interceptación de las comunicaciones o de las telecomunicaciones a una serie de delitos graves, en reconocimiento de la privacidad de las comunicaciones y de las telecomunicaciones verbales y al carácter intrusivo de esta medida de investigación. Del mismo modo, este Convenio sólo exige que las Partes establezcan poderes y procedimientos de intervención en relación con los datos del contenido de las comunicaciones informáticas especificas en relación con una serie de delitos graves que serán determinados por la legislación nacional.

143. En segundo lugar, una Parte puede reservarse el derecho de aplicar las medidas previstas en el Artículo 20 (obtención en tiempo real de datos relativos al tráfico) sólo a aquellos delitos o categorías de delitos especificados en la reserva, siempre que la serie de dichos delitos o categoría de delitos no sea más restringida que la serie de delitos a los que corresponde aplicar las medidas de interceptación contempladas en el Artículo 21. Algunos Estados consideran que la obtención de datos relativos al tráfico es equivalente a la obtención de datos relativos al contenido por lo que se refiere a la privacidad y a su carácter intrusivo. El derecho a formular una reserva permitiría a esos Estados limitar la aplicación de las medidas para obtener en tiempo real datos relativos al tráfico a la misma serie de delitos a los que se aplican los poderes y procedimientos de interceptación en tiempo real de los datos relativos al contenido. Sin embargo, muchos Estados consideran que la interceptación de los datos relativos al contenido no es

equivalente a la obtención de datos relativos al tráfico por lo que respecta a la privacidad y el grado de intrusión, ya que la obtención de los datos relativos al tráfico por sí solos no permite obtener ni revelar el contenido de la comunicación. Como la obtención en tiempo real de los datos relativos al tráfico puede ser muy importante para remontar hasta la fuente o averiguar el destino de las comunicaciones informáticas (lo que contribuye a identificar a los delincuentes), el Convenio invita a aquellas Partes que ejerzan su derecho a formular una reserva a que limiten dicha reserva, con el fin de permitir una aplicación lo más amplia posible de los poderes y procedimientos establecidos para obtener en tiempo real datos relativos al tráfico.

144. El apartado b) prevé la posibilidad de que las Partes formulen una reserva cuando, a causa de las restricciones que impongan su legislación vigente en el momento de la adopción de este Convenio, no puedan interceptar comunicaciones en los sistemas informáticos que se hayan puesto en funcionamiento para un grupo restringido de usuarios, que no empleen las redes públicas de telecomunicaciones y que no estén conectados a otros sistemas informáticos. El término "grupo restringido de usuarios" se refiere, por ejemplo, a un conjunto de usuarios que está limitado por asociación con un proveedor de servicios, como puede ser el caso de los empleados de una empresa a los que se ofrece la posibilidad de comunicarse entre sí a través de la red informática de la empresa. La expresión "no esté conectado a otro sistema informático" quiere decir que, en el momento en que se emitiera una orden en virtud de los Artículos 20 y 21, el sistema en el que se transmiten las comunicaciones no tiene una conexión física o lógica con otra red informática. La expresión "no emplea redes públicas de telecomunicación" excluye los sistemas que utilizan redes informáticas de uso público (incluido Internet), redes telefónicas públicas u otros servicios públicos de telecomunicaciones para la transmisión de las comunicaciones, sea o no este uso evidente para los usuarios.

Condiciones y salvaguardias (Artículo 15)

145. La instauración, ejecución y aplicación de los poderes y procedimientos previstos en esta Sección del Convenio estarán sometidos a las condiciones y salvaguardias previstas en el derecho interno de cada Parte. Si bien las Partes están obligadas a introducir ciertas disposiciones de derecho procesal en sus leyes nacionales, las modalidades del establecimiento y la aplicación de esos poderes y procedimientos en sus sistemas jurídicos y la aplicación de los poderes y procedimientos en casos específicos estarán sujetas a las leyes y los procedimientos nacionales de cada Parte. Esas leyes y procedimientos internos, tal como se describe más concretamente a continuación, deberán incluir condiciones o salvaguardias, las que pueden ser provistas constitucionalmente, legislativamente, judicialmente o de otra manera. Las modalidades deberían incluir la adición de ciertos elementos como las condiciones y salvaguardias destinados a lograr un equilibrio entre los

requisitos de aplicación de la ley y la protección de los derechos y libertades humanas. Como el Convenio se aplica a Partes que tienen diferentes sistemas jurídicos y culturas muy diversas, no es posible especificar en detalle las condiciones y salvaguardias aplicables a cada poder o procedimiento. Las Partes deberán velar por que estas condiciones y salvaguardias brinden la adecuada protección de los derechos y las libertades humanas. Existen algunas normas comunes o salvaguardias mínimas a las que las Partes de este Convenio deben adherir. Estas incluyen las normas o salvaguardias mínimas que se deriven de las obligaciones contraídas por una Parte en virtud de los instrumentos internacionales aplicables en materia de derechos humanos. Estos instrumentos incluyen el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950) y sus Protocolos adicionales núm. 1, 4, 6, 7 y 12 (STE núm. 005[4], 009, 046, 114, 117 y 177), respecto de los Estados europeos que sean Partes en los mismos. Incluyen también otros instrumentos aplicables en materia de derechos humanos respecto de Estados que se encuentran en otras regiones (por ejemplo, la Convención Americana Sobre Derechos Humanos (1969) y la Carta Africana sobre Derechos Humanos y de los Pueblos (1981), que sean Partes en estos instrumentos, así como también el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966), cuya ratificación es más universal. Además, las leyes de la mayoría de los Estados prevén protecciones similares.

146. Otra salvaguardia incluida en el Convenio es que las competencias y procedimientos deberán "integrar el principio de proporcionalidad". Este principio deberá ser aplicado por cada Parte, con arreglo a los principios pertinentes de su derecho interno. Por lo que respecta a los países europeos, esto se deriva de los principios del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y las Libertades Fundamentales (1950), de su jurisprudencia aplicable y de las leyes y la jurisprudencia de cada país, que establecen que el poder o procedimiento deberá ser proporcional a la naturaleza y las circunstancias del delito. Otros Estados aplicarán los principios correspondientes contemplados en sus leyes, tales como las limitaciones respecto del alcance de las órdenes de presentación de información y de los requisitos sobre la aceptabilidad de las órdenes de registro y confiscación. Además, la limitación explícita contenida en el Artículo 21 que prevé que las obligaciones relativas a las medidas de

[4] El texto del Convenio ha sido modificado de conformidad con las disposiciones del Protocolo núm. 3 (STE núm. 45), que entró en vigor el 21 de septiembre de 1970, del Protocolo núm. 5 (STE núm. 55), que entró en vigor el 20 de diciembre de 1971 y del Protocolo núm. 8 (STE núm. 118), que entró en vigor el 1 de enero de 1990, y ha integrado también el texto del Protocolo núm. 2 (STE núm. 44) que, de conformidad con el artículo 5, párrafo 3, había sido una parte integral del Convenio desde su entrada en vigor el 21 de septiembre de 1970. Todas las disposiciones que se han modificado o añadido por esos Protocolos han sido sustituidas por el Protocolo núm. 11 (STE núm. 155), a partir de la fecha de su entrada en vigor el 1 de noviembre de 1998. A partir de esa fecha, el Protocolo núm. 9 (STE núm. 140), que entró en vigor el 1 de octubre de 1994, quedó derogado y el Protocolo núm. 10 (STE núm. 146) ha perdido su razón de ser.

interceptación relativas a una serie de delitos graves, deberán definirse en el derecho interno de cada país, constituye un ejemplo explícito de la aplicación del principio de proporcionalidad.

147. Sin limitar los tipos de condiciones y salvaguardias que pudieran ser aplicables, el Convenio estipula específicamente que tales condiciones y salvaguardias, teniendo en cuenta la naturaleza del poder o procedimiento de que se trate, deberán incluir una supervisión judicial, u otra forma de supervisión independiente; los motivos que justifiquen su aplicación, y una limitación respecto del ámbito de aplicación y de la duración de dicho poder o procedimiento. Las asambleas legislativas nacionales deberán determinar, al aplicar los compromisos internacionales vinculantes y los principios nacionales establecidos, cuáles poderes y procedimientos son lo suficientemente intrusivos por naturaleza para requerir la aplicación de condiciones y salvaguardias adicionales. Como se establece en el párrafo 215, las Partes deberían aplicar condiciones y salvaguardias claras de este tipo por lo que respecta a la interceptación, habida cuenta de su carácter intrusivo. Al mismo tiempo, por ejemplo, no es necesario que dichas salvaguardias se apliquen de igual manera a la conservación. Otras salvaguardias que deberían preverse en las leyes nacionales incluyen el derecho contra la autoinculpación, los privilegios jurídicos y la especificidad de las personas o lugares que sean objeto de la aplicación de la medida.

148. Con respecto a las cuestiones discutidas en el párrafo 3, reviste primordial importancia tener en cuenta el "interés público", en particular, los intereses de "la buena administración de la justicia". Siempre que sea conforme con el interés público, las Partes deberían considerar otros factores, tales como el impacto que el poder o procedimiento pudiera tener sobre "los derechos, responsabilidades e intereses legítimos de terceros", incluidos los proveedores de servicios, como resultado de la aplicación de las medidas, y si cabe emplear medios apropiados para mitigar dicho impacto. En síntesis, se da consideración inicial a la buena administración de la justicia, los intereses públicos (por ej., la seguridad pública y la salud pública) y otros intereses (por ej., los intereses de las víctimas y el respeto a la vida privada). En la medida en que sean conformes con el interés público, se deberían considerar también cuestiones como la minimización de la interrupción de los servicios a los consumidores, la exención de responsabilidad por revelar o facilitar la revelación de información a que hace referencia este capítulo, o la protección de intereses patrimoniales.

Título 2 - Conservación rápida de datos informáticos almacenados

149. Las medidas contenidas en los Artículos 16 y 17 se aplican a los datos almacenados ya obtenidos y conservados por los titulares de los datos, como, por ej., los proveedores de servicios. No se aplican a la obtención en tiempo real y a la conservación de los datos relativos al tráfico en el futuro ni

al acceso en tiempo real a los contenidos de las comunicaciones. Estas cuestiones se abordan en el Título 5.

150. Las medidas descritas en los artículos se aplican sólo a datos informáticos que ya existen y están almacenados. Debido a muchas razones, podría ocurrir que los datos informáticos pertinentes para las investigaciones penales no existieran o no estuvieran almacenados. Por ejemplo, pudiera no haberse recogido ni conservado datos precisos, o si hubieran sido recogidos, podrían no haber sido conservados. Las leyes sobre la protección de los datos pudieran haber exigido la destrucción de datos importantes antes de que alguien se percatara de su importancia para los procedimientos penales. En algunos casos puede no existir ninguna razón comercial para obtener y conservar datos, como ocurre cuando los clientes abonan una tarifa plana por los servicios o cuando los servicios son gratuitos. Estos problemas no se abordan en los Artículos 16 y 17.

151. El término "conservación de datos" debe distinguirse de la " retención de datos". Si bien ambas expresiones tienen significados similares en el lenguaje común, tienen distintos significados en relación con el uso de los ordenadores. Conservar los datos significa guardar los datos, que ya están almacenados de algún modo, protegiéndolos contra cualquier cosa que pudiera causar una modificación o deterioro de su calidad o condición actual. Retener datos significa guardar a partir de este momento los datos que están siendo generados en este momento. La retención de los datos implica acumular datos en el presente y guardarlos o mantener su posesión en el futuro. La retención de los datos es el proceso de almacenar datos. Por el contrario, la conservación de los datos es la actividad destinada a guardar los datos almacenados de manera segura.

152. Los Artículos 16 y 17 se refieren únicamente a la conservación de datos, y no a la retención de datos. No imponen la obtención y retención de todos, ni incluso de algunos, de los datos recopilados por un proveedor de servicios u otra entidad en el curso de sus actividades. Las medidas referentes a la conservación se aplican a los datos informáticos que "han sido almacenados por medio de un sistema informático", lo que supone que los datos ya existen, se han obtenido y están almacenados. Además, como se indica en el Artículo 14, todos los poderes y procedimientos que la Sección 2 del Convenio exige establecer son "a los efectos de investigación o de procedimientos penales específicos", que limitan la aplicación de las medidas a una investigación que se realiza en un caso en particular. Además, cuando una Parte emite una orden en que solicita medidas de conservación, ésta debe ser en relación a "determinados datos informáticos almacenados que se encuentren en poder o bajo el control de esa persona" (párrafo 2). Por consiguiente, los artículos prevén sólo la facultad de exigir la conservación de datos almacenados existentes, quedando pendiente la posterior revelación de los datos en consideración de otras facultades jurídicas, en relación con investigaciones o procedimientos penales específicos.

153. La obligación de asegurar la conservación de los datos no tiene por objeto exigir a las Partes que restrinjan la oferta o el uso de los servicios que no recopilan ni conservan habitualmente ciertos tipos de datos, tales como los datos relativos al tráfico o los datos de los abonados, como parte de sus prácticas comerciales legítimas. Tampoco exige que los mismas implanten nuevas capacidades técnicas para hacerlo, por ej., para preservar datos efímeros, que pueden estar presentes en el sistema por un período tan breve que podía no ser razonable conservarlos en respuesta a una solicitud o una orden.

154. Algunos Estados tienen leyes que requieren que ciertos tipos de datos, como es el caso de los datos personales en poder de determinados tipos de titulares de datos no sean conservados y que sean borrados si su conservación ya no persigue una finalidad comercial. En la Unión Europea, el principio general está previsto en la Directiva 95/46/CE y, en el contexto particular del sector de las telecomunicaciones, en la Directiva 97/66/CE. Esas directivas establecen la obligación de eliminar los datos tan pronto como su almacenamiento ya no sea necesario. Sin embargo, los Estados miembros podrán adoptar leyes para establecer excepciones en los casos necesarios con el fin de prevenir, investigar o iniciar acciones respecto de un delito penal. Estas directivas no impiden que los Estados miembros de la Unión Europea establezcan poderes y procedimientos conforme a lo previsto en su derecho interno con el fin de preservar determinados datos para investigaciones específicas.

155. Para la mayoría de los países, la conservación de los datos es una facultad o procedimiento judicial totalmente nuevo en el derecho interno. Es una nueva e importante herramienta de investigación para hacer frente a los delitos informáticos y los delitos relacionados con la informática, especialmente los delitos cometidos a través de Internet. En primer lugar, debido a la volatilidad de los datos informáticos, éstos son fácilmente objeto de manipulaciones y modificaciones. Por lo tanto, valiosas pruebas de un delito pueden desaparecer fácilmente debido a negligencias en el manejo o las prácticas de almacenamiento; a la manipulación o borrado deliberados de los datos con el fin de destruir las pruebas, o a la eliminación sistemática de datos cuya conservación no se requiere por más tiempo. Un método de preservar la integridad de los datos es que las autoridades competentes registren, o accedan de manera similar, y confisquen, o consigan de manera similar, los datos necesarios. Sin embargo, cuando los datos están bajo la custodia de alguien de confianza, tal como una empresa de renombre, la integridad de los datos puede preservarse más rápidamente con una orden de conservación de datos. Para las empresas legítimas, una orden de conservación de datos puede representar también un menor perjuicio para sus actividades normales y su reputación que el efectuar un registro y confiscación en sus instalaciones. En segundo lugar, los delitos informáticos y los delitos relacionados con el uso de los ordenadores son cometidos en gran medida como resultado de la transmisión de comunicaciones a través de un sistema informático. Estas comunicaciones pueden contener contenidos

ilegales, tales como pornografía infantil, virus informáticos u otras instrucciones que causen interferencias con los datos o con el correcto funcionamiento del sistema informático, o pruebas de la comisión de otros delitos, tales como el narcotráfico o el fraude. Determinar el origen o el destino de esas comunicaciones pasadas puede contribuir a determinar la identidad de los autores de los delitos. Con el fin de rastrear esas comunicaciones a fin de determinar su origen o destino, es necesario obtener datos relativos al tráfico relacionados con esas comunicaciones pasadas (véase la explicación adicional respecto de la importancia de los datos relativos al tráfico en el Artículo 17 *infra*). En tercer lugar, cuando estas comunicaciones vehiculan contenidos ilícitos o pruebas de una actividad delictiva y los proveedores de servicios conservan copias de dichas comunicaciones como, por ej., los mensajes de correo electrónico, es importante proceder a la conservación de esas comunicaciones a fin de asegurar que no desaparezcan pruebas esenciales. Obtener copias de esas comunicaciones pasadas (por ej., los mensajes de correo electrónico enviados o recibidos que estén almacenados) puede revelar pruebas de un acto delictivo.

156. La facultad de requerir la conservación rápida de los datos informáticos se propone abordar esas cuestiones. Por consiguiente, las Partes deberán adoptar las medidas que resulten necesarias para la conservación de determinados datos informáticos como medida provisional, durante el tiempo necesario, hasta un máximo de 90 días. Una Parte puede prever la renovación de dicha orden. Esto no significa que los datos son revelados a las autoridades encargadas de la aplicación de la ley en el momento en que se procede a su conservación. Para obtener su revelación, es necesaria una medida adicional de revelación de los datos o un registro. Con respecto a la revelación de los datos preservados a las autoridades, véanse los párrafos 152 y 160.

157. También es importante que existan medidas de conservación a nivel nacional con el fin de permitir a las Partes prestarse asistencia mutua en el plano internacional por lo que se refiere a la conservación rápida de datos almacenados que se encuentren en sus respectivos territorios. Esto contribuirá a impedir que los datos esenciales desaparezcan durante los prolongados procedimientos de asistencia jurídica mutua que permiten a la Parte requerida obtener realmente los datos y revelarlos a la Parte requirente.

Conservación rápida de datos informáticos almacenados (Artículo 16)

158. El artículo 16 tiene por objeto garantizar que las autoridades nacionales competentes puedan ordenar, o de manera similar obtener, la conservación rápida de datos informáticos específicos almacenados en el marco de una investigación o procedimiento penal específico.

159. La “conservación” requiere que los datos, que ya existen y están almacenados de alguna forma, sean protegidos contra todo lo que pudiera causar que su calidad o condición actual sufriera un cambio o deterioro. Requiere que sean guardados a salvo de toda modificación, deterioro o eliminación. La conservación no significa necesariamente que los datos sean "congelados" (es decir, sean inaccesibles) y que los mismos, o copias de los mismos, no puedan ser utilizados por sus legítimos usuarios. La persona a quien va dirigida la orden puede, en función de las especificaciones exactas de la orden, seguir accediendo a los datos. El artículo no especifica la manera en que han de conservarse los datos. Queda a criterio de cada Parte determinar la manera de conservación apropiada y, en los casos en que proceda, si la conservación de los datos debiera también llevar a su “congelación”.

160. La referencia a “ordenar o imponer de otro modo” tiene como finalidad permitir el uso de otros métodos jurídicos para lograr la conservación además de una orden judicial o administrativa o de una directiva (por ej., de la policía o el fiscal). El derecho procesal de algunos Estados no contempla las órdenes de conservación, por lo que la conservación y obtención de los datos requiere una orden de registro y confiscación, o de presentación de información. El uso de la frase "o imponer de otro modo” ofrece cierta flexibilidad a los Estados para que apliquen este artículo empleando estos medios. Sin embargo, se recomienda que los Estados consideren el establecimiento de poderes y procedimientos que permitan ordenar efectivamente al receptor de la orden de conservación de los datos que actúe con la mayor celeridad posible para lograr la rápida aplicación de las medidas de conservación en determinados casos.

161. El poder para ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos se aplica a todo tipo de datos informáticos almacenados. Ello puede incluir cualquier tipo de datos que estén especificados en la orden de conservación de datos. Puede incluir, por ejemplo, registros comerciales, de salud, personales o de otra índole. Las Partes deben establecer medidas que se utilizarán "en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación." Ello puede incluir situaciones en que los datos sean objeto de un breve período de conservación, tal como ocurre cuando una empresa tiene la política de eliminar los datos después de un cierto período de tiempo o cuando los datos son borrados habitualmente cuando el medio de almacenamiento es utilizado para grabar otros datos. También puede referirse a la naturaleza de quien custodia los datos o a la manera insegura en que se almacenan los datos. Sin embargo, si quien los custodia no fuera digno de confianza, sería más seguro lograr su conservación mediante registro y confiscación, en lugar de enviar una orden que podría no ser obedecida. En el párrafo 1 figura una referencia expresa a "los datos relativos al tráfico" con el fin de señalar la particular aplicabilidad de las disposiciones a ese tipo de datos, los cuales cuando son recopilados y conservados por un proveedor de servicios, en general se guardan solo por

poco tiempo. Asimismo, la referencia a los "datos relativos al tráfico" establece un vínculo entre las medidas que figuran en los Artículos 16 y 17.

162. El párrafo 2 especifica que cuando una Parte imparta una orden de conservación de datos, dicha orden ha de ser en relación a "determinados datos almacenado que se encuentren en poder o bajo el control de esa persona". Así, los datos almacenados pueden realmente estar en posesión de una persona o estar almacenados en otro lugar, aunque estando sujetos al control de esa persona. La persona a quien está dirigida la orden tiene la obligación de "conservar y proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de 90 días, con el fin de que las autoridades competentes puedan obtener su revelación". La legislación nacional de cada Parte debería especificar el plazo máximo durante el cual deberán conservarse los datos objeto de una orden, y ésta debería especificar el tiempo exacto durante el que deberán conservarse los datos especificados. El lapso de tiempo debería ser tan largo como fuera necesario, hasta un máximo de 90 días, con el fin de que las autoridades competentes puedan recurrir a otras medidas legales, tales como el registro y la confiscación, o el acceso por un medio similar, o impartir una orden de presentación de información, para obtener la revelación de los datos. Una Parte puede prever la renovación de la orden de presentación de información. En este contexto, debería recordarse lo dispuesto en el Artículo 29 con relación a una solicitud de asistencia mutua para obtener la conservación rápida de los datos almacenados por medio de un sistema informático. En aquel artículo se especifica que las medidas de conservación adoptadas en respuesta a solicitudes de asistencia mutua "serán válidas por un período mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, o la revelación de los datos".

163. El párrafo 3 impone la obligación de mantener en secreto la ejecución de los procedimientos de conservación a la persona que custodia los datos o a otra persona encargada de su conservación durante el tiempo previsto en su derecho interno. Ello requiere que las Partes adopten medidas para garantizar el secreto respecto de la conservación rápida de los datos almacenados y fijen el límite de tiempo en que se debe mantener el secreto. Esta medida da cuenta de las necesidades de las autoridades encargadas de la aplicación de las leyes para que el sospechoso de la investigación no tenga conocimiento de la misma, al igual que del derecho de las personas al respeto de la vida privada. Para las autoridades encargadas de la aplicación de las leyes, la conservación rápida de los datos forma parte de las investigaciones iniciales, por lo que puede ser importante mantener el secreto en esa etapa. La conservación es una medida preliminar en espera de la adopción de otras medidas legales para la obtención o la revelación de los datos. El secreto es necesario para evitar que otras personas intenten alterar o borrar los datos. Para la persona a quien va dirigida la orden, el sujeto de los datos u otras personas que pudieran estar mencionadas o identificadas en los datos, existe un plazo máximo respecto de la duración de

la medida. La doble obligación de guardar los datos de manera segura y de mantener el secreto sobre el hecho que se ha efectuado la medida de conservación contribuye a proteger la vida privada del sujeto de los datos o de otras personas que pudieran estar mencionadas o identificadas en los datos.

164. Además de las limitaciones expuestas más arriba, las poderes y procedimientos contemplados en el Artículo 16 están también sujetos a las condiciones y salvaguardias establecidas en los Artículos 14 y 15.

Conservación y revelación parcial rápidas de los datos relativos al tráfico (Artículo 17)

165. Este artículo establece obligaciones específicas en relación con la conservación de los datos relativos al tráfico en aplicación del Artículo 16, y establece la revelación rápida de algunos datos relativos al tráfico con el fin de identificar a los proveedores de servicios que estuvieron involucrados en la transmisión de las comunicaciones especificadas. Los "datos relativos al tráfico" se definen en el Artículo 1.

166. La obtención de los datos relativos al tráfico almacenados correspondientes a comunicaciones pasadas puede ser esencial para determinar el origen o el destino de las comunicaciones realizadas, elemento crucial para identificar a las personas que han distribuido, por ej., pornografía infantil, información fraudulenta como parte de un plan fraudulento o virus informáticos, o que han intentado acceder o han accedido ilegalmente a sistemas informáticos, o que han transmitido comunicaciones a un sistema informático causando interferencias, ya sea a los datos contenidos en el sistema o a su correcto funcionamiento. Sin embargo, se debe señalar que en muchos casos esos datos se almacenan sólo por cortos períodos de tiempo; ello puede obedecer a que las leyes de protección de la vida privada prohíben el almacenamiento de dichos datos, o a que las fuerzas del mercado no alientan el almacenamiento de dichos datos por mucho tiempo. Por consiguiente, es importante que se tomen medidas de conservación destinadas a garantizar la integridad de esos datos (véase *supra* la discusión relativa a la conservación).

167. En muchos casos puede estar involucrado en la transmisión de una comunicación más de un proveedor de servicios. Cada proveedor de servicios puede poseer algunos datos relativos al tráfico relacionados con la transmisión de una comunicación específica, que han sido generados y conservados por ese proveedor de servicios en relación con el tránsito de la comunicación por su sistema o que han sido aportados por otros proveedores de servicios. A veces los datos relativos al tráfico, o al menos algunos tipos de datos relativos al tráfico, se comparten entre los proveedores de servicios involucrados en la transmisión de la comunicación con fines comerciales, de

seguridad o técnicos. En tal caso, cualquiera de los proveedores de servicios puede poseer los datos relativos al tráfico que son esenciales para determinar el origen o el destino de la comunicación. Sin embargo, en muchos casos no hay ningún proveedor de servicios que posea la suficiente cantidad de datos esenciales relativos al tráfico para poder determinar el origen real o el destino de la comunicación. Cada uno posee una parte del rompecabezas, y es necesario examinar cada una de estas partes para identificar el origen o el destino de la comunicación.

168. El Artículo 17 garantiza que pueda llevarse a cabo la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de una comunicación. El artículo no especifica los medios que pueden emplearse, dejando a criterio de la legislación nacional de cada país determinar una forma que sea coherente con sus sistemas jurídico y económico. Una manera de lograr la conservación rápida sería que las autoridades competentes presentaran con rapidez a cada proveedor de servicio órdenes individuales de conservación de los datos. Con todo, la obtención de una serie de órdenes individuales puede tomar demasiado tiempo. Una alternativa preferible podría ser obtener una sola orden, que pudiera ser aplicable a todos los proveedores de servicios que posteriormente se determine que han participado en la transmisión de una comunicación determinada. Esa orden global podría presentarse de forma secuencial a cada uno de los proveedores de servicios especificados. Otras alternativas posibles podrían implicar la participación de los proveedores de servicios. Por ejemplo, se podría exigir a un proveedor de servicios que recibe una orden de conservación de datos que notifique al siguiente proveedor de servicios de la cadena respecto de la existencia y los términos de dicha orden. Dependiendo de las leyes de cada país, ese aviso podría tener como efecto permitir que el siguiente proveedor de servicios conservase de manera voluntaria los correspondientes datos relativos al tráfico, a pesar de cualquier obligación que pudiera existir para borrarlos, o imponer la conservación de los correspondientes datos relativos al tráfico. El segundo proveedor de servicios podría notificar de manera similar al siguiente proveedor de servicios de la cadena.

169. Como los datos relativos al tráfico no son revelados a las autoridades encargadas de aplicar las leyes cuando se envía una orden de conservación de datos a un proveedor de servicios (sino que se obtienen o revelan solo más tarde después de que se han tomado otras medidas jurídicas), las autoridades no pueden saber si el proveedor de servicios posee todos los datos esenciales relativos al tráfico o si otros proveedores de servicios participaron en la transmisión de la comunicación. Por consiguiente, este artículo dispone que el proveedor de servicios que recibe una orden de conservación de datos, o una medida similar, revele con prontitud a las autoridades competentes, o a otra persona designada, un volumen suficiente de datos relativos al tráfico que permita a las autoridades competentes identificar tanto a los proveedores de servicios como la vía por la cual se transmitió la comunicación. Las autoridades competentes deberían

especificar con claridad el tipo de datos relativos al tráfico que deben ser revelados. La recepción de esa información permitiría a las autoridades competentes determinar si es necesario tomar medidas de conservación respecto de otros proveedores de servicios. De este modo, las autoridades encargadas de la investigación pueden rastrear la comunicación para determinar su origen o su destino, e identificar al autor, o autores, del delito concreto que se investiga. Las medidas que figuran en este Artículo están también sujetas a las limitaciones, condiciones y salvaguardias previstas en los Artículos 14 y 15.

Título 3 - Orden de presentación

Orden de presentación (Artículo 18)

170. En el párrafo 1 de este artículo se insta a las Partes a que faculten a sus autoridades competentes a ordenar a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder, o a ordenar a un proveedor que ofrezca sus servicios en el territorio de dicha Parte a que suministre información relativa a los abonados. Los datos en cuestión son los datos almacenados o existentes, y no incluyen aquellos que todavía no se han generado, tales como los datos relativos al tráfico o los datos relativos al contenido con respecto a comunicaciones futuras. En lugar de exigir que los Estados apliquen sistemáticamente medidas coercitivas en relación con terceros, tales como el registro y la confiscación de datos, es esencial que los Estados incluyan en su derecho interno facultades de investigación alternativas que proporcionen medios menos intrusivos para obtener información relevante para las investigaciones penales.

171. Una "orden de presentación" representa una medida flexible que las autoridades encargadas de hacer cumplir la ley pueden aplicar en muchos casos, especialmente en lugar de otras medidas que son más invasivos o más onerosas. La aplicación de este tipo de mecanismo procesal también será beneficiosa para los terceros encargados de la custodia de los datos, tales como los ISP, que a menudo están dispuestos a ayudar en forma voluntaria a las autoridades encargadas de hacer cumplir las leyes suministrando los datos que están bajo su control, pero que prefieren que exista una base jurídica adecuada para esa asistencia, que los libere de toda responsabilidad tanto contractual como no contractual.

172. La orden de presentación se refiere a datos informáticos o a información sobre los abonados que obren en poder o estén bajo el control de una persona o de un proveedor de servicios. La medida es aplicable sólo en la medida en que la persona o el proveedor de servicios mantenga los correspondientes datos o información. Algunos proveedores de servicios, por ejemplo, no conservan registros de sus abonados.

173. Conforme a lo dispuesto en el párrafo 1.a), una de las Partes garantizará que sus autoridades competentes tengan la facultad de ordenar a una persona que se encuentre en su territorio que comunique determinados datos informáticos que obren en su poder o estén bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento de datos. La expresión "obren en su poder o estén bajo su control" se refiere a la posesión física de los datos en cuestión en el territorio de la Parte que imparta la orden y también a situaciones en las cuales la persona no tenga la posesión física de los datos que deben presentarse, pero que dicha persona pueda, no obstante, controlar libremente la presentación de los mismos desde dentro del territorio de la Parte que imparte la orden (por ejemplo, sujeto a los privilegios aplicables, una persona que recibe una orden de presentación de la información almacenada en su cuenta por medio de un servicio de almacenamiento en línea a distancia tiene la obligación de presentar esa información). Al mismo tiempo, la mera capacidad técnica para acceder remotamente a datos almacenados (por ejemplo, la capacidad que tiene un usuario para acceder a distancia a través de un enlace de red a datos almacenados que no están bajo su control legítimo) no constituye necesariamente "control" con arreglo al significado de esta disposición. En algunos Estados, el concepto denominado "posesión" en derecho abarca la posesión física y constructiva y es lo suficientemente amplio para satisfacer el requisito de que los datos estén "en su poder o bajo su control".

En virtud de lo dispuesto en el párrafo 1.b), las Partes deberán prever también la facultad de ordenar a un proveedor de servicios que ofrece servicios en su territorio a que "comunique los datos que obren en su poder o estén bajo su control relativos a los abonados". Al igual que en el párrafo 1.a), la expresión "que obren en su poder o estén bajo su control" se refiere a información sobre los abonados que el proveedor de servicios posea físicamente y a información sobre los abonados almacenada remotamente que está bajo el control del proveedor de servicios (por ejemplo, en una instalación remota de almacenamiento de datos provista por otra compañía). La expresión "en relación con dichos servicios" quiere decir que se otorgará esa facultad con el fin de obtener información acerca de los abonados en relación con servicios ofrecidos en el territorio de la Parte que ordena la presentación de los datos.

174. En función del derecho interno de cada Parte, las condiciones y salvaguardias contempladas en el párrafo 2 de este Artículo pueden excluir datos o información privilegiada. Una Parte podría desear prescribir diferentes términos, diferentes autoridades competentes y diversas salvaguardias en cuanto a la presentación de determinados tipos de datos informáticos o de información sobre los abonados que esté en posesión de ciertas categorías de personas o de proveedores de servicios. Por ejemplo, con respecto a algunos tipos de datos como la información sobre los abonados disponible públicamente, una Parte podría autorizar que dicha orden sea impartida por los agentes encargados de hacer cumplir las leyes cuando en otras situaciones sería necesaria una orden judicial. Por el

contrario, en algunas situaciones una Parte podría exigir, o estar obligada a exigir en virtud de salvaguardias respecto de los derechos humanos, que la orden de presentación de información sea impartida únicamente por las autoridades judiciales tratándose de la obtención de ciertos tipos de datos. Las Partes podrían desear restringir la revelación de esos datos a aquellas situaciones en que la orden de presentación de información ha sido impartida por las autoridades judiciales. El principio de proporcionalidad prevé también cierta flexibilidad en relación con la aplicación de la medida, por ejemplo, en muchos Estados, a fin de excluir su aplicación en los casos de menor cuantía.

175. Otra consideración que pueden hacer las Partes es la posible inclusión de medidas relativas a la confidencialidad. La disposición no contiene una referencia específica a la confidencialidad, a fin de mantener el paralelismo con el mundo no electrónico, donde por lo general no se impone el secreto respecto de las órdenes de presentación de información. Sin embargo, en el mundo electrónico, particularmente en el mundo en línea, una orden de presentación de información puede a veces ser empleada como una medida preliminar en la investigación, precediendo a otras medidas tales como el registro y la confiscación o la interceptación en tiempo real de otros datos. El secreto podría ser esencial para el éxito de la investigación.

176. Por lo que respecta a las distintas modalidades de presentación de la información, las Partes podrían establecer la obligación de que los datos informáticos especificados o la información sobre los abonados sea presentada de la manera especificada en la orden. Ello podría incluir una referencia al período de tiempo en el cual se debe efectuar la revelación, o al formato, por ej., que los datos o la información se presenten en "texto plano", en línea, impresa en papel o en disquete.

177. La expresión "datos relativos a los abonados" se define en el párrafo 3. En principio, abarca cualquier tipo de información que posea un proveedor de servicios y que se refiera a los abonados de sus servicios. La información relativa a los abonados puede consistir tanto en datos informáticos como en información que puede estar en cualquier otro formato como, por ej., los registros impresos. Dado que la información relativa a los abonados incluye otras formas de datos y no sólo los informáticos, se ha incluido una disposición especial en el artículo para dar cuenta de este tipo de información. El término "abonado" abarca a una amplia gama de clientes del proveedor de servicios, e incluye a quienes tienen abonos pagos, aquellos que pagan en función del uso que hacen, y los que reciben los servicios en forma gratuita. También incluye la información respecto de las personas que tienen derecho a utilizar la cuenta del abonado.

178. En el curso de una investigación penal, la información relativa a los abonados puede ser necesaria mayormente en dos situaciones específicas. En primer lugar, la información relativa a los abonados es necesaria para determinar los servicios y las medidas técnicas que han sido utilizadas o están siendo utilizados por un abonado, tales como el tipo de servicio

telefónico utilizado (por ej., móvil), los diferentes servicios conexos utilizados (por ejemplo, desvío de llamadas, buzón de voz, etc.), el número de teléfono u otra dirección técnica (por ej., la dirección de correo electrónico). En segundo lugar, cuando se conoce una dirección técnica, es necesario tener la información relativa al abonado para poder establecer la identidad de la persona en cuestión. Otra información relativa a los abonados, tal como la información comercial sobre los registros de facturación y los pagos de los abonados también pueden ser relevantes para las investigaciones penales, especialmente cuando el delito que se investiga está relacionado con el fraude informático u otros delitos económicos.

179. Por consiguiente, la información relativa a los abonados incluye varios tipos de información en cuanto al uso de un servicio y al usuario de dicho servicio. Por lo que respecta a la utilización del servicio, el término abarca cualquier tipo de información, con excepción de los datos relativos al tráfico o al contenido, que permita determinar el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo durante el cual una persona estuvo abonada al servicio. El término "disposiciones técnicas" incluye todas las medidas adoptadas para hacer posible que un abonado disfrute del servicio de comunicación ofrecido. Dichas disposiciones incluyen la reserva de un número o una dirección técnica (número de teléfono, dirección de un sitio web o nombre de dominio, dirección de correo electrónico, etc.), así como también la provisión y el registro de los equipos de comunicaciones utilizados por el abonado, tales como los teléfonos, las centrales telefónicas o las redes de área local.

180. La información relativa al abonado no está limitada a la información directamente relacionada con el uso del servicio de comunicación. También abarca cualquier información, excepto los datos relativos al tráfico o los datos relativos al contenido, que permita establecer la identidad del usuario, su dirección postal o ubicación geográfica, el número de teléfono o cualquier otro número de acceso, y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicios entre el abonado y el proveedor de servicios. Abarca también cualquier otra información, excepto los datos relativos al tráfico o al contenido, relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicios. Este último tipo de información puede ser relevante en términos prácticos sólo cuando el equipo no es móvil, pero el conocimiento en cuanto a la movilidad o supuesta ubicación de los equipos (sobre la base de la información proporcionada en virtud de un contrato o un acuerdo de prestación de servicios) puede ser muy útil para una investigación.

181. Sin embargo, no debería entenderse que este Artículo impone la obligación a los proveedores de servicios para que mantengan registros de sus abonados, ni tampoco exige a los proveedores de servicios que se aseguren de la exactitud de dicha información. Así, un proveedor de servicios

no está obligado a registrar la información referente a la identidad de los usuarios de las denominadas tarjetas de prepago para los servicios de telefonía móvil. Tampoco está obligado a verificar la identidad de los abonados o a rechazar el uso de seudónimos por parte de los usuarios de sus servicios.

182. Como los poderes y procedimientos previstos en esta Sección están orientados a llevar a cabo investigaciones o procedimientos penales (Artículo 14), las órdenes de presentación de información han de ser utilizadas en casos particulares que guardan relación, por lo general, con determinados abonados. Por ejemplo, la divulgación de un determinado nombre mencionado en la orden de presentación, puede llevar a solicitar el número de teléfono o la dirección de correo electrónico correspondientes. El conocimiento de un determinado número de teléfono o dirección de correo electrónico, puede llevar a ordenar que se de a conocer el nombre y la dirección del abonado en cuestión. La disposición no autoriza a las Partes a dictar una orden judicial destinada a revelar cantidades indiscriminadas de información relativa a los abonados del proveedor de servicios respecto de grupos de usuarios, por ejemplo con el fin de proceder a una extracción sistemática de datos ("*data-mining*").

183. La referencia a un "contrato o un acuerdo de prestación de servicios" debe interpretarse en un sentido amplio e incluye todo tipo de relación que permite a un cliente utilizar los servicios del proveedor.

Título 4 – Registro y confiscación de datos informáticos almacenados

Registro y confiscación de datos informáticos almacenados (Artículo 19)

184. Este artículo tiene como finalidad modernizar y armonizar las leyes nacionales respecto del registro y la confiscación de los datos informáticos almacenados a efectos de obtener pruebas relacionadas con investigaciones y procedimientos penales específicos. El derecho procesal penal de todos los países incluye poderes de registro y confiscación de objetos tangibles. Sin embargo, en algunas jurisdicciones los datos informáticos almacenados *per se* no se consideran un objeto tangible y, en consecuencia, no pueden ser obtenidos en el marco de una investigación o procedimiento penal haciendo un paralelismo con los objetos tangibles, excepto mediante la confiscación del soporte de la información en que está almacenada. La finalidad del Artículo 19 del presente Convenio es establecer una facultad equivalente respecto de los datos almacenados.

185. En el entorno de un allanamiento tradicional en relación con documentos o registros, se trata de reunir pruebas que han sido grabadas o registradas en el pasado en forma tangible, por ej., impresos en papel. Los investigadores proceden al allanamiento e inspeccionan dichos datos

registrados, confiscando o secuestrando físicamente el registro tangible. La recogida de datos tiene lugar durante el allanamiento y guarda relación con los datos existentes en ese momento. La condición previa para obtener la autoridad legal para llevar a cabo un allanamiento es la existencia de razones para creer, conforme a lo que establecen las leyes nacionales y las salvaguardias de los derechos humanos, que dichos datos existen en un lugar en particular y que pueden servir de prueba respecto de un delito penal concreto.

186. Con respecto al registro para encontrar pruebas, en particular datos informáticos, en el nuevo entorno tecnológico, se siguen dando muchas de las características de un allanamiento tradicional. Por ejemplo, la obtención de los datos se lleva a cabo durante el allanamiento y guarda relación con datos que existen en ese momento. Las condiciones previas para la obtención de la autoridad legal para realizar un allanamiento siguen siendo las mismas. El grado de certeza requerido para obtener una autorización legal para efectuar un registro no es diferente, tanto si los datos están en forma tangible o en forma electrónica. Del mismo modo, las razones y el registro tienen que ver con datos que ya existen y que proporcionarán pruebas sobre un delito específico.

187. Sin embargo, por lo que respecta al registro en busca de datos informáticos, son necesarias nuevas disposiciones procesales a fin de garantizar la obtención de los datos informáticos de una manera que sea igualmente eficaz a la del registro y confiscación de un soporte de datos tangibles. Hay varias razones para ello: en primer lugar, los datos se encuentran en forma intangible como, por ej., en forma electromagnética. En segundo lugar, si bien los datos pueden ser leídos con el uso de equipos informáticos, no pueden ser confiscados y secuestrados de la misma manera que cuando se trata de un registro impreso. El medio físico en el que están almacenados los datos intangibles (por ej., el disco duro de un ordenador o un disquete) deben ser confiscados y secuestrados, o se debe hacer una copia de los datos, ya sea en forma tangible (por ej., una copia impresa de los datos informáticos) o en forma intangible en un medio físico (por ej., una disquete), antes de poder confiscar y secuestrar el medio tangible que contiene la copia. En las dos últimas situaciones, cuando se hacen copias de los datos, una copia de los datos queda en el sistema informático o en el dispositivo de almacenamiento. Las leyes de cada país deberían prever la facultad necesaria para hacer tales copias. En tercer lugar, debido a la manera en que están conectados los sistemas informáticos, los datos pueden no estar almacenados en el ordenador específico que es revisado, pero esos datos pueden ser de fácil acceso para dicho sistema. Podrían estar almacenados en un dispositivo conexo de almacenamiento de datos conectado directamente al ordenador o indirectamente a través de sistemas de comunicación, tales como Internet. Ello puede o no requerir nuevas leyes para permitir una extensión del registro hasta llegar al punto en que los datos estén efectivamente almacenados (o la recuperación de los datos de ese sitio en el ordenador que es objeto del registro), o el uso de las

facultades tradicionales de allanamiento de una manera más coordinada y expedita en ambos lugares.

188. El párrafo 1 dispone que las Partes faculten a las autoridades competentes para registrar o tener acceso a los datos informáticos que se encuentren tanto dentro de un sistema informático como en una parte del mismo (tal como un dispositivo de almacenamiento de datos que esté conectado), o en un medio de almacenamiento de datos independiente (como un CD-ROM o disquete). Como la definición de "sistema informático" en el Artículo 1 se refiere a "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí", el párrafo 1 tiene que ver con el registro de todo sistema informático y sus componentes conexos que pueda considerarse que forman parte de un sistema informático claramente identificable (por ejemplo, un PC con una impresora y los correspondientes dispositivos de almacenamiento, o una red de área local). A veces se puede acceder legalmente a datos que se encuentran almacenados físicamente en otro sistema o dispositivo de almacenamiento al cual se puede acceder legalmente desde el sistema informático allanado estableciendo una conexión con otros sistemas informáticos distintos. Esta situación, que involucra enlaces con otros sistemas informáticos por medio de redes de telecomunicaciones dentro del mismo territorio (por ejemplo, red de área extensa o Internet), se aborda en el párrafo 2.

189. Si bien el registro y la confiscación de un dispositivo "de almacenamiento informático que permita almacenar datos informáticos" (Artículo 19, párrafo 1.b)) puede llevarse a cabo con arreglo a las facultades tradicionales de registro judicial, en muchos casos el registro de un ordenador requiere el allanamiento tanto del sistema informático como de todo medio conexo de almacenamiento de datos informáticos (por ejemplo, disquetes) que se encuentren en las inmediaciones del sistema informático. Debido a esta relación, en el párrafo 1 se prevé una facultad jurídica amplia que abarca ambas situaciones.

190. El Artículo 19 se aplica a los datos informáticos almacenados. Respecto de esto, se plantea la cuestión de si un mensaje de correo electrónico no abierto que se encuentra en el buzón de entrada de mensajes de un proveedor de Internet hasta que el destinatario lo descargue a su sistema informático, debe considerarse datos informáticos almacenados, o datos en proceso de transferencia. Conforme a las leyes de algunas Partes, ese mensaje de correo electrónico es parte de una comunicación y, por consiguiente, su contenido sólo puede obtenerse aplicando la facultad de interceptación; por el contrario, otros sistemas jurídicos consideran dicho mensaje como datos almacenados a los que corresponde aplicar el Artículo 19. Por consiguiente, las Partes deberían analizar su legislación respecto de esta cuestión para determinar lo que es apropiado con arreglo a sus respectivos ordenamientos jurídicos.

191. Se hace referencia a la expresión "registrar o tener acceso de un modo similar". El uso de la palabra tradicional "registrar" da la idea de que el Estado ejerce una facultad coercitiva, e indica que la facultad mencionada en este artículo es análoga al allanamiento tradicional. "Registrar" supone buscar, leer, inspeccionar o revisar datos. Incluye los conceptos de búsqueda de datos y de revisión (examen) de datos. Por otro lado, la palabra "acceso" tiene un sentido neutro, pero refleja más adecuadamente la terminología informática. Se utilizan ambos términos con el fin de vincular los conceptos tradicionales con la terminología moderna.

192. La referencia a "en su territorio" es un recordatorio de que esta disposición, al igual que todos los artículos en esta Sección, conciernen sólo a medidas que es necesario tomar a nivel nacional.

193. El párrafo 2 permite a las autoridades encargadas de la investigación ampliar su registro o el acceso de un modo similar a otro sistema informático o parte del mismo si tienen motivos para creer que los datos buscados se hallan almacenados en ese otro sistema. No obstante, el otro sistema informático, o una parte del mismo, debe también estar situado "en su territorio".

194. El Convenio no establece la manera en que se permitirá o llevará a cabo la extensión de un registro. Ello dependerá del derecho interno de cada país. Entre las posibles condiciones cabe destacar algunos ejemplos: facultar a la autoridad judicial o de otro tipo que haya autorizado el registro de un sistema informático específico a que autorice la extensión del registro o el acceso de modo similar a un sistema conectado si tuviera motivos para creer (en la medida en que lo exigen las leyes nacionales y las salvaguardias de los derechos humanos) que el sistema informático conectado puede contener los datos específicos que se están buscando; facultar a las autoridades encargadas de las investigaciones a extender el registro autorizado, o el acceso de modo similar, de un sistema informático específico a un sistema informático conectado cuando existan motivos similares para creer que los datos específicos que se buscan están almacenados en el otro sistema informático; o ejercer las facultades para proceder al registro, o acceder de manera similar, a ambos lugares en forma coordinada y rápida. En todos los casos, los datos objeto del registro deben estar legalmente accesibles desde el sistema informático inicial o estar disponibles en ese sistema.

195. Este artículo no aborda la cuestión del "registro y la confiscación transnacionales", que permite a los Estados allanar y secuestrar datos que se encuentren en territorio de otros Estados sin tener que pasar por los canales habituales de la asistencia mutua. Esta cuestión se analiza más adelante en el capítulo sobre la cooperación internacional.

196. El párrafo 3 dispone que las Partes adoptarán medidas para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1

ó 2. Esas medidas incluyen la prerrogativa de confiscar equipos informáticos y dispositivos de almacenamiento de datos. En ciertos casos, por ejemplo, cuando los datos están almacenados en sistemas operativos únicos, por lo que no se pueden copiar, es inevitable confiscar el dispositivo de almacenamiento de los datos en su totalidad. Esto también puede ser necesario cuando es necesario almacenar el dispositivo de almacenamiento de datos a fin de recuperar antiguos datos sobre los que se han grabado posteriormente otros datos pero que, sin embargo, han dejado trazas en el dispositivo de almacenamiento de los datos.

197. En el presente Convenio, "confiscar" significa secuestrar el medio físico en el cual están grabados los datos o la información, o hacer y conservar una copia de dichos datos o información. "Confiscar" incluye el uso o la incautación de los programas necesarios para acceder a los datos que se han confiscado. Además del término tradicional de "confiscar" se incluye el término "obtener de un modo similar" para dar cuenta de otros medios por los cuales los datos intangibles se extraen, se prohíbe su acceso, o se adquiere su control de otro modo en el entorno informático. Dado que las medidas se refieren a datos intangibles almacenados, es necesario que las autoridades competentes adopten medidas adicionales para salvaguardar los datos, es decir, "preservar la integridad de los datos", o mantener la "cadena de custodia" de los datos, lo que significa que los datos copiados o extraídos serán conservados en el Estado en que fueron encontrados en el momento de la confiscación y permanecerán inalterados mientras duren los procedimientos penales. El término se refiere a tomar el control sobre los datos o el apoderarse de los datos.

198. El prohibir el acceso a los datos puede incluir el cifrado de los datos, u otra forma de frenar por medios tecnológicos el acceso a esos datos. Esta medida podría ser aplicada provechosamente en situaciones donde pudiera existir peligro o perjuicio para la sociedad, como ocurre con los programas de virus o las instrucciones para crear virus o hacer bombas, o cuando los datos o sus contenidos sean ilegales, como ocurre con la pornografía infantil. El término "suprimir" se propone recoger la idea de que si bien los datos se suprimen, o se prohíbe el acceso a los mismos, los datos no han sido destruidos, sino que siguen existiendo. El sospechoso se encuentra temporalmente privado de ellos, pero pueden serles devueltos al término de las investigaciones o los procedimientos penales.

199. Así el hecho de confiscar datos, u obtenerlos de un modo similar, tiene dos funciones: 1) reunir pruebas, por ej., mediante la copia de los datos, o 2) confiscar los datos, por ej., copiando los datos y más tarde haciendo inaccesible la versión original de los datos o borrándolos. La confiscación no implica la supresión definitiva de los datos confiscados.

200. El párrafo 4 introduce una medida coercitiva para facilitar el registro y la confiscación de datos informáticos. Aborda del problema práctico de la dificultad para acceder a los datos que se desea obtener como prueba e

identificarlos, en vista del volumen de datos que pueden ser tratados y almacenados, el uso de medidas de seguridad y la naturaleza de las operaciones informáticas. Reconoce que puede ser necesario consultar a los administradores de los sistemas, que tienen conocimientos particulares de esos sistemas, para determinar la manera más adecuada de llevar a cabo el registro. Por consiguiente, esta disposición permite a las autoridades competentes obligar a un administrador de sistema a que brinde ayuda, dentro de límites razonables, en cuanto al registro y la confiscación.

201. Los beneficios de esta facultad no están limitados solamente a las autoridades que llevan a cabo la investigación. Sin ese tipo de cooperación, esas autoridades podrían permanecer en los locales allanados e impedir el acceso al sistema informático durante mucho tiempo, mientras proceden al registro. Ello podría representar una carga económica para las empresas, clientes y abonados legítimos a los que se les niega el acceso a los datos durante ese tiempo. Una facultad que permita ordenar la cooperación de personas que tienen conocimientos en la materia haría más eficaces y económicos esos registros, tanto para las autoridades competentes como para las personas inocentes que se ven afectadas. El obligar legalmente al administrador de un sistema a prestar su ayuda puede también descargar al administrador de toda obligación contractual o de otra índole respecto de la divulgación de los datos.

202. Se puede ordenar la presentación de aquella información que sea necesaria para hacer posible el registro y la confiscación, o para tener acceso de un modo similar a los datos. Sin embargo, la presentación de esa información está limitada a lo que se considere "razonable". En algunas circunstancias, la presentación razonable puede incluir la revelación de una contraseña u otra medida de seguridad a las autoridades encargadas de la investigación. Sin embargo, esto podría no ser razonable en otras circunstancias, por ejemplo, cuando la divulgación de la contraseña u otra medida de seguridad pudiera poner en peligro injustificadamente la vida privada de otros usuarios o de otros datos cuya revisión no ha sido autorizada. En tal caso, el suministro de la información "necesaria" podría consistir en la revelación, en una forma que sea comprensible y legible, de los datos que realmente andan buscando las autoridades competentes.

203. En virtud del párrafo 5 de este artículo, las medidas están sujetas a las condiciones y salvaguardias previstas en el derecho interno de cada país como dispone el Artículo 15 de este Convenio. Dichas condiciones pueden incluir disposiciones relativas a la participación y la compensación financiera de los testigos y peritos.

204. Quienes redactaron el Convenio debatieron asimismo, en el marco del párrafo 5, si las partes interesadas deberían ser informadas de que se lleva a cabo un procedimiento de registro. En el mundo en línea puede ser menos evidente que se ha procedido a un registro y confiscación (copia) de datos que cuando se lleva a cabo un secuestro en el mundo real, cuando los

objetos incautados se decomisan físicamente. El derecho interno de algunas Partes no establece la obligación de notificar tratándose de un allanamiento tradicional. Si el convenio requiriese la notificación del registro de un sistema informático, se crearía una discrepancia con las leyes de esas Partes. Por el contrario, algunas Partes pueden considerar que la notificación es una característica esencial de la medida, destinada a mantener la distinción entre registro y confiscación de datos almacenados en ordenador (que en general no pretende ser una medida subrepticia) e interceptación del flujo de datos (que es una medida subrepticia, véanse los Artículos 20 y 21). Por consiguiente, la cuestión de la notificación dependerá de lo que disponga la legislación nacional. Si las Partes consideran necesario contar con un sistema de notificaciones obligatorias a las personas involucradas, se debería tener presente que las notificaciones pueden perjudicar la investigación. Si existiera dicho riesgo, debería considerarse la posibilidad de aplazar la notificación.

Título 5 – Obtención en tiempo real de datos informáticos

205. Los Artículos 20 y 21 prevén la obtención en tiempo real de datos relativos al tráfico y la interceptación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas por un sistema informático. Las disposiciones dan cuenta de la obtención en tiempo real y la interceptación en tiempo real de dichos datos por parte de las autoridades competentes, así como también la obtención o interceptación por parte de los proveedores de servicios. También se abordan las obligaciones de confidencialidad.

206. La interceptación de las telecomunicaciones por lo general tiene que ver con las redes tradicionales de telecomunicaciones. Dichas redes pueden incluir infraestructuras de cable, tanto alámbricas como de fibra óptica, así como interconexiones con redes inalámbricas, incluidos los sistemas de telefonía móvil y los sistemas de transmisión por microondas. Hoy en día, las comunicaciones móviles también recurren a un sistema de redes satelitales especiales. Las redes informáticas pueden tener también una infraestructura fija independiente por cable, pero más frecuentemente funcionan como una red virtual que depende de conexiones efectuadas a través de las infraestructuras de telecomunicaciones, lo que permite crear redes informáticas, o enlaces de redes, de naturaleza global. La distinción entre las telecomunicaciones y las comunicaciones informáticas, y la distinción entre sus infraestructuras, está tornándose borrosa debido a la convergencia de las telecomunicaciones y las tecnologías de la información. Es por ello que la definición de "sistema informático" en el Artículo 1 no restringe la manera en la cual pueden estar interconectados los dispositivos, o grupos de dispositivos. Por consiguiente, los Artículos 20 y 21 se refieren a comunicaciones específicas transmitidas por medio de un sistema informático, lo que podría incluir la transmisión de la comunicación a través

de redes de telecomunicaciones antes de ser recibida por otro sistema informático.

207. Los Artículos 20 y 21 no establecen ninguna distinción entre un sistema de telecomunicaciones o un sistema informático de carácter público o privado, ni entre la utilización de sistemas y servicios de comunicación ofrecidos al público o a grupos restringidos de usuarios o partes privadas. La definición de "proveedor de servicios" en el Artículo 1 se refiere a las entidades públicas y privadas que brindan a los usuarios de sus servicios la posibilidad de comunicarse por medio de un sistema informático.

208. Este Título rige la obtención de pruebas contenidas en comunicaciones que se están generando en este momento, que son obtenidas en el momento en que se produce la comunicación (es decir, "en tiempo real"). Los datos son intangibles en cuanto a su forma (por ej., en forma de transmisiones de voz o de impulsos electrónicos). El flujo de los datos no se ve interferido significativamente por las medidas adoptadas para la obtención de los datos y la comunicación llega a su destinatario. En lugar de un secuestro físico de los datos, se realiza una grabación (es decir, una copia) de los datos que se están transmitiendo. La obtención de esas pruebas se lleva a cabo durante un determinado período de tiempo. Se solicita autorización legal para permitir la obtención respecto de un acontecimiento futuro (es decir, la transmisión futura de datos).

209. Se pueden obtener dos tipos de datos: los datos relativos al tráfico y los datos relativos al contenido. De acuerdo con la definición del Artículo 1.d se entiende por "datos relativos al tráfico" todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por éste último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. En el Convenio no se define el término "datos relativos al contenido", pero éste se refiere al contenido comunicativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o información transmitidos por la comunicación (excepto los datos relativos al tráfico).

210. En muchos Estados se hace una distinción entre la interceptación en tiempo real de datos relativos al contenido y la obtención en tiempo real de datos relativos al tráfico, tanto por lo que se refiere a los requisitos legales que deben cumplirse para que se autorice tal medida de investigación como a los delitos respecto de los cuales se puede emplear esta medida. Si bien se reconoce que ambos tipos de datos llevan aparejados intereses relativos al respeto de la vida privada, muchos Estados consideran que la cuestión del respeto de la vida privada es más importante por lo que respecta a los datos relativos al contenido debido a la índole del contenido o del mensaje de la comunicación. Puede que se impongan mayores limitaciones con respecto a la obtención en tiempo real de los datos relativos al contenido que a los datos relativos al tráfico. Para contribuir a reconocer la distinción que existe

en esos Estados, el Convenio, si bien reconoce a nivel operativo que en ambas situaciones se obtienen o registran datos, se refiere normativamente en los títulos de los artículos a la obtención de los datos relativos al tráfico como "obtención en tiempo real" y a la obtención de los datos relativos al contenido como "interceptación en tiempo real".

211. En algunos Estados la legislación vigente no establece distinción alguna entre la obtención de datos relativos al tráfico y la interceptación de datos relativos al contenido, ya sea porque en las leyes no se ha hecho ninguna distinción por lo que refiere a las diferencias que existen en cuanto al respeto de la vida privada, o porque el aspecto tecnológico de las técnicas de obtención de datos son muy similares en ambos casos. Por lo tanto, los requisitos legales que se deben cumplir para que se pueda autorizar el empleo de esas medidas, y los delitos respecto de los cuales cabe emplear las medidas, son idénticos. Esta situación también se reconoce en el Convenio mediante el uso común a nivel operativo de la expresión "obtener o grabar" en el texto de ambos Artículos 20 y 21.

212. En lo tocante a la interceptación en tiempo real de datos relativos al contenido, en muchos casos la ley establece que la medida es aplicable solo en relación con la investigación de delitos graves o de categorías de delitos graves. Estos delitos están definidos en el derecho interno de cada país como graves para este fin, y a menudo figuran en una lista de delitos aplicables o están incluidos en esta categoría porque se hace referencia a la sentencia máxima de prisión que es aplicable al delito. Por lo tanto, por lo que respecta a la interceptación de los datos relativos al contenido, el Artículo 21 dispone específicamente que solo se requiere que las Partes establezcan esa medida "en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno".

213. Por otro lado, el Artículo 20, relativo a la obtención de datos relativos al tráfico, no está sujeto a ese tipo de limitación y, en principio, se aplica a todo delito penal comprendido en el Convenio. Sin embargo, el Artículo 14, párrafo 3, establece que una Parte puede reservarse el derecho de aplicar la medida sólo a aquellos delitos o categorías de delitos especificados en la reserva, siempre que la serie de delitos o de categorías de delitos no sea más restringida que la serie de delitos a los que se aplica la medida de interceptación de los datos relativos al contenido. No obstante, cuando se formule ese tipo de reserva, la Parte deberá considerar restringir esa reserva para permitir la más amplia gama de aplicación de la medida relativa a la obtención de los datos relativos al tráfico.

214. Algunos Estados podrían normalmente considerar que los delitos establecidos en el Convenio no son lo suficientemente graves como para permitir la interceptación de datos relativos al contenido o, en algunos casos, incluso la obtención de datos relativos al tráfico. Sin embargo, dichas técnicas a menudo revisten una importancia crucial para la investigación de algunos de los delitos establecidos en el Convenio, tales como los

relacionados con el acceso ilícito a sistemas informáticos, y la distribución de virus y de pornografía infantil. Por ejemplo, en algunos casos no es posible determinar la fuente de la intrusión o la distribución sin obtener en tiempo real datos relativos al tráfico. En algunos casos, no es posible descubrir la naturaleza de la comunicación sin la interceptación en tiempo real de los datos relativos al contenido. Estos delitos, por su naturaleza o por el medio de transmisión, implican la utilización de tecnologías informáticas. Por consiguiente, debería estar permitido el empleo de medios tecnológicos en la investigar de los mismos. Con todo, como la interceptación de datos relativos al contenido es un tema delicado, el Convenio deja que el ámbito de aplicación de esta medida se determine atendiendo a lo dispuesto en el derecho interno. En vista de que algunos países asimilan desde el punto de vista legal la obtención de datos relativos al tráfico con la interceptación de datos relativos al contenido, se permite la posibilidad de que puedan formular una reserva con el fin de restringir la aplicabilidad de la disposición anterior, cuya amplitud no deberá ser superior a la de la restricción impuesta por la Parte en cuanto a la interceptación en tiempo real de los datos relativos al contenido. Sin embargo, las Partes deberían considerar la aplicación de ambas medidas a los delitos establecidos por el Convenio en la Sección 1 del Capítulo II, con el fin de contar con un medio eficaz para la investigación de estos delitos informáticos y los delitos relacionados con la informática.

215. Las condiciones y salvaguardias respecto de los poderes y procedimientos relacionados con la interceptación en tiempo real de los datos relativos al contenido y la obtención en tiempo real de los datos relativos al tráfico están sujetas a lo dispuesto en los Artículos 14 y 15. Como la interceptación de los datos relativos al contenido es una medida muy intrusiva en la vida privada, se requieren salvaguardias rigurosas para garantizar un equilibrio adecuado entre los intereses de la justicia y los derechos fundamentales de las personas. En el ámbito de la interceptación, el presente Convenio no establece salvaguardias específicas aparte de limitar la autorización de la interceptación de los datos relativos al contenido a aquellas investigaciones que guarden relación con los delitos graves definidos en el derecho interno de cada país. Sin embargo, las siguientes condiciones y salvaguardias importantes en esta área, aplicadas en las leyes nacionales, son: la supervisión judicial u otro tipo de supervisión independiente; la especificidad respecto de las comunicaciones o las personas a ser interceptadas, la necesidad, subsidiaridad y proporcionalidad (por ej., los fundamentos jurídicos que justifiquen la adopción de la medida; la ineficacia de otras medidas menos intrusivas); una limitación respecto de la duración de la interceptación, el derecho a una compensación. Muchas de estas salvaguardias reflejan lo dispuesto en el Convenio Europeo de Derechos Humanos y su jurisprudencia posterior (véanse las sentencias en los casos Klass[5], Kruslin[6], Huvig[7], Malone[8], Halford[9] y Lambert[10]). Algunas de estas

5 Sentencia del CEDH en el caso de Klass y otros contra Alemania, A28, 06/09/1978.

6 Sentencia del CEDH en el caso de Kruslin contra Francia, 176-A, 24/04/1990.

salvaguardias son aplicables también a la obtención en tiempo real de los datos relativos al tráfico.

Obtención en tiempo real de datos relativos al tráfico (Artículo 20)

216. En muchos casos, los datos históricos relativos al tráfico pueden ya no estar disponibles o pueden no ser pertinentes, ya que el intruso ha cambiado la ruta de comunicación. Por lo tanto, la obtención en tiempo real de datos relativos al tráfico es una importante medida en la investigación. El Artículo 20 aborda el tema de la obtención en tiempo real y de la grabación de datos relativos al tráfico en cuanto a investigaciones y procedimientos penales específicos.

217. Tradicionalmente, la obtención de datos relativos al tráfico respecto de las telecomunicaciones (por ej., las conversaciones telefónicas) ha sido una herramienta de investigación útil para determinar el origen o el destino (por ej., los números de teléfono) y datos conexos (por ej., hora, fecha y duración) de diversos tipos de comunicaciones ilegales (por ej., amenazas, hostigamientos, conspiración, tergiversaciones fraudulentas) y de comunicaciones que aportan pruebas de delitos pasados o futuros (por ej., tráfico de drogas, asesinatos, delitos económicos, etc.)

218. Las comunicaciones informáticas pueden constituir o aportar pruebas respecto de los mismos tipos de delitos. Sin embargo, como la tecnología informática es capaz de transmitir grandes volúmenes de datos, incluidos textos e imágenes visuales y sonoras, también se presta más para la comisión de delitos que impliquen la distribución de contenidos ilegales (por ej., la pornografía infantil). Del mismo modo, como los ordenadores son capaces de almacenar grandes cantidades de datos, a menudo de índole privada, el potencial para causar un perjuicio, ya sea económico, social o personal, puede ser significativo si se interfiere con la integridad de estos datos. Además, como la ciencia de la tecnología informática está basada en el procesamiento de los datos, en cuanto producto final y como parte de su función operativa (por ej., la ejecución de programas informáticos), cualquier interferencia con esos datos puede acarrear efectos desastrosos para el buen funcionamiento de los sistemas informáticos. Cuando ocurre distribución ilegal de pornografía infantil, acceso ilícito a un sistema informático o interferencia con el buen funcionamiento del sistema informático o la integridad de los datos, especialmente a distancia, como por ej., a través de Internet, es necesario y crucial rastrear la ruta de las comunicaciones remontándonos desde la víctima hasta el autor del delito. Por lo tanto, la

---

7 Sentencia del CEDH en el caso de Huvig contra Francia, 176-B, 24/04/1990.

8 Sentencia del CEDH en el caso de Malone contra el Reino Unido, A82, 02/08/1984.

9 Sentencia del CEDH en el caso de Halford contra el Reino Unido, los informes de 1997 - III, 25/06/1997.

10 Sentencia del CEDH en el caso de Lambert c. Francia, Informes, 1998 - V, 24/08/1998.

capacidad para obtener datos relativos al tráfico con respecto a las comunicaciones informáticas es tan importante, si no más, que la relativa a las telecomunicaciones puramente tradicionales. Esta técnica de investigación permite correlacionar la hora, la fecha, el origen y el destino de las comunicaciones efectuadas por el sospechoso con la hora de las intrusiones a los sistemas de las víctimas, identificar a otras víctimas o demostrar vínculos con los cómplices.

219. En virtud de este Artículo, los datos relativos al tráfico que se desee obtener deben estar asociados con comunicaciones especificas en el territorio de la Parte. Se habla de "comunicaciones" especificas en plural, porque pudiera ser necesario obtener datos relativos al tráfico respecto de diversas comunicaciones a fin de identificar a las personas en su origen o destino (por ejemplo, en una casa donde varias personas utilizan las mismas instalaciones de telecomunicaciones, puede ser necesario establecer una correlación entre varias comunicaciones y las oportunidades que tuvieron esas personas para utilizar el sistema informático). Con todo, deberán especificarse las comunicaciones respecto de las cuales se pueden obtener o registrar datos relativos al tráfico. Así, el Convenio no exige, ni autoriza la vigilancia y obtención generalizada o indiscriminada de grandes volúmenes de datos relativos al tráfico. No autoriza las "expediciones de pesca", en las que se abriga la esperanza de descubrir actividades delictivas, a diferencia de los casos concretos de delitos que se están investigando. La orden judicial o de otro tipo que autoriza la obtención de datos debe especificar las comunicaciones cuyos datos se desea obtener.

220. Sujeto a lo dispuesto en el párrafo 2, las Partes están obligadas, en virtud del párrafo 1.a) a garantizar que sus autoridades competentes tengan la capacidad para obtener o registrar datos relativos al tráfico empleando medios técnicos. El artículo no especifica cómo se han de obtener desde el punto de vista tecnológico, y no se definen obligaciones en términos técnicos.

221. Además, en virtud del párrafo 1.b), las Partes están obligadas a garantizar que sus autoridades competentes están facultadas para obligar a un proveedor de servicios a obtener o registrar datos relativos al tráfico, o de cooperar y ayudar a las autoridades competentes para obtener o grabar esos datos. Esa obligación respecto de los proveedores de servicios es aplicable sólo en la medida en que la obtención o la grabación, o la cooperación y la asistencia, transcurran dentro de los límites de la capacidad técnica existente del proveedor de servicios. El artículo no obliga a los proveedores de servicios a asegurarse de que tienen la capacidad técnica para obtener o grabar esos datos, o para brindar cooperación o asistencia. No requiere que adquieran o desarrollen nuevos equipos, contraten expertos o realicen una costosa reconfiguración de sus sistemas. Sin embargo, si sus sistemas y el personal tienen ya la capacidad técnica necesaria para obtener o grabar esos datos, o para brindar cooperación o asistencia, el artículo exigiría que los proveedores tomaran las medidas necesarias para comprometer esa capacidad. Por ejemplo, el sistema puede estar configurado de cierta

manera, o el proveedor de servicios podría disponer ya de los programas informáticos necesarios que hagan posible tomar tales medidas que, por lo general, no se llevan a cabo en el curso de las operaciones normales del proveedor de servicios. El artículo requeriría que el proveedor de servicios comprometiera, o activara, dichas características, como exige la ley.

222. Como ésta es una medida que se lleva a cabo a nivel nacional, las medidas se aplican a la obtención o grabación de determinadas comunicaciones en el territorio de una Parte. En consecuencia, en la práctica, las obligaciones son de aplicación general cuando el proveedor de servicios cuenta con cierta infraestructura física o equipos capaces de llevar a cabo las medidas en ese territorio, aunque éste no sea la sede de sus oficinas y operaciones principales. A los efectos del presente Convenio, se entiende que una comunicación se encuentra en el territorio de una Parte si una de las Partes que se comunican (seres humanos o equipos) se encuentra en su territorio o si el equipo informático o de telecomunicaciones a través del cual pasa la comunicación se encuentra en su territorio.

223. En general, las dos posibilidades para recopilar datos relativos al tráfico en los apartados a) y b) del párrafo 1 no son alternativas. Salvo lo dispuesto en el párrafo 2, las Partes deben garantizar que ambas medidas puedan llevarse a cabo. Esto es necesario porque si un proveedor de servicios no posee la capacidad técnica para obtener o grabar los datos relativos al tráfico (1 b)), una de las Partes deberá tener entonces la posibilidad de que se encarguen de ello sus autoridades competentes (1.a)). Del mismo modo, la obligación que se deriva del inciso ii) del párrafo 1 b) para cooperar y ayudar a las autoridades competentes en la obtención o la grabación de los datos relativos al tráfico no tiene sentido si las autoridades competentes no están facultadas para obtener o grabar ellas mismas los datos relativos al tráfico. Además, en los casos de algunas redes de área local (LAN), en las que pudiera no estar involucrado ningún proveedor de servicios, la única manera de obtener o grabar los datos sería que las autoridades encargadas de la investigación lo hagan ellas mismas. No es necesario que en todos los casos se recurra a ambas medidas previstas en los párrafos 1 a) y b), pero el artículo exige que estén disponibles ambos métodos.

224. Sin embargo, esa doble obligación plantea dificultades para ciertos Estados en los cuales las autoridades competentes sólo estaban facultadas para interceptar datos en los sistemas de telecomunicaciones mediante la ayuda del proveedor de servicios, y no subrepticiamente sin que al menos tuviera conocimiento de ello el proveedor de servicios. Por este motivo, el párrafo 2 contempla tal situación. Cuando una Parte no pueda adoptar las medidas contempladas en el párrafo 1.a) "por respeto a los principios establecidos en su ordenamiento jurídico interno", podrá, en su lugar adoptar un enfoque diferente como, por ej., el de sólo obligar a los proveedores de servicios a proveer las instalaciones técnicas necesarias para asegurar la obtención o grabación en tiempo real de datos relativos al tráfico por parte de las autoridades competentes. En tal caso, se seguirán aplicando todas las

demás limitaciones respecto del territorio, la especificidad de las comunicaciones y la utilización de medios técnicos.

225. Al igual que ocurre con la interceptación en tiempo real de datos relativos al contenido, la obtención en tiempo real de datos relativos al tráfico sólo es eficaz si se lleva a cabo sin el conocimiento de las personas que están siendo investigadas. La interceptación es subrepticia y debe llevarse a cabo de manera tal que las partes que se comunican no se percaten de lo que está ocurriendo. Por consiguiente, los proveedores de servicios y sus empleados que tengan conocimiento de la interceptación deben cumplir con la obligación de guardar el secreto a fin de que el procedimiento pueda llevarse a cabo de manera eficaz.

226. El párrafo 3 obliga a las Partes a adoptar las medidas legislativas y de otro tipo que sean necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto. Esta disposición no sólo asegura la confidencialidad de la investigación, sino que también descarga al proveedor de servicios de toda obligación contractual o legal para notificar a los abonados que se están recopilando datos sobre ellos. El párrafo 3 puede verse afectado por la creación de obligaciones explícitas que estén contenidas en las leyes. Por otra parte, una Parte puede ser capaz de asegurar la confidencialidad de la medida sobre la base de otras disposiciones legales nacionales, tales como la facultad de iniciar acciones por obstrucción de la justicia contra las personas que ayuden a los delincuentes informándoles respecto de la medida. Si bien es preferible como procedimiento contar con la obligación específica de mantener la confidencialidad (con sanciones efectivas en caso de una violación), el uso del delito de obstrucción de la justicia puede ser un medio alternativo para evitar la revelación inapropiada y, por lo tanto, también es suficiente para la aplicación de este párrafo. Cuando se crean obligaciones explícitas de confidencialidad, éstas deberán estar sujetas a las condiciones y salvaguardias previstas en los artículos 14 y 15. Esas salvaguardias o condiciones deberían imponer plazos razonables respecto de la duración de la obligación, dada la naturaleza subrepticia de la investigación.

227. Como se señaló más arriba, por lo general se considera que el interés por el respeto de vida privada menos es menos marcado en lo tocante a la obtención de los datos relativos al tráfico que con respecto a la interceptación de los datos relativos al contenido. Los datos relativos al tráfico que tienen que ver con la hora, la duración y el tamaño de la comunicación revelan poca información personal acerca de una persona o su manera de pensar. Sin embargo, el respeto del derecho a la vida privada puede ser considerado una cuestión más importante por lo que se refiere a los datos sobre el origen o el destino de una comunicación (por ej., los sitios web visitados). La obtención de esos datos puede permitir, en ciertos casos, tener un perfil de los intereses de una persona, de sus asociados y de su contexto social. En consecuencia, las Partes deberían tener en cuenta esas

consideraciones al establecer las salvaguardias y los requisitos legales apropiados a la hora de emprender esas medidas, de conformidad con lo dispuesto en los Artículos 14 y 15.

Interceptación de datos relativos al contenido (Artículo 21)

228. Tradicionalmente, la recogida de datos relativos al contenido respecto de las telecomunicaciones (por ej., las conversaciones telefónicas) ha sido una herramienta de investigación útil para determinar que la comunicación es de carácter ilegal (por ejemplo, la comunicación constituye acoso o una amenaza criminal, una conspiración criminal o tergiversaciones fraudulentas), y para reunir pruebas sobre delitos pasados y futuros (por ej., tráfico de drogas, asesinatos, delitos económicos, etc.). Las comunicaciones informáticas pueden constituir o aportar pruebas respecto de los mismos tipos de delitos. Sin embargo, como la tecnología informática permite transmitir grandes cantidades de datos, incluidos textos, imágenes visuales y sonoras, tiene un mayor potencial para cometer delitos que impliquen la distribución de contenidos ilegales (por ej., pornografía infantil). Muchos de los delitos informáticos implican la transmisión o la comunicación de datos como ocurre con las comunicaciones enviadas para efectuar un acceso ilícito a un sistema informático o la distribución de virus informáticos. No es posible determinar en tiempo real el carácter nocivo e ilegal de estas comunicaciones sin interceptar el contenido del mensaje. Sin la capacidad para determinar y prevenir la comisión de un delito en curso, la aplicación de las leyes quedaría limitada meramente a los delitos investigados y completados en el pasado, cuando el daño ya ha ocurrido. Por lo tanto, la interceptación en tiempo real de los datos relativos al contenido de las comunicaciones informáticas es tan, o más, importante como la interceptación en tiempo real de las telecomunicaciones.

229. Por “datos relativos al contenido" se entiende el contenido comunicativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o la información transmitida por la comunicación. Se trata de todo lo transmitido como parte de la comunicación que no sean datos relativos al tráfico.

230. La mayoría de los elementos de este artículo son idénticos a los del Artículo 20. Por lo tanto, los comentarios que figuran más arriba respecto de la obtención o la grabación de datos relativos al tráfico, la obligación de cooperar y brindar ayuda y las obligaciones de confidencialidad, se aplican igualmente a la interceptación de datos relativos al contenido. Debido al mayor interés por el respeto de la vida privada en el caso de los datos relativos al contenido, la medida de investigación se limita a "un repertorio de delitos graves que deberá definirse en su derecho interno".

231. Además, como se indica en las observaciones anteriores sobre el Artículo 20, las condiciones y salvaguardias aplicables a la interceptación en

tiempo real de datos relativos al contenido pueden ser más rigurosas que las aplicables a la obtención en tiempo real de datos relativos al tráfico, o al registro y confiscación, o al acceso por medios similares, de los datos almacenados.

Sección 3 – Jurisdicción

Jurisdicción (Artículo 22)

232. Este Artículo establece una serie de criterios en virtud de los cuales las Partes Contratantes están obligadas a afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio.

233. El acápite a) del párrafo 1 está basado en el principio de territorialidad. Cada Parte tiene la obligación de castigar la comisión de los delitos establecidos en este Convenio que sean cometidos en su territorio. Por ejemplo, una Parte haría valer su jurisdicción territorial, si tanto la persona que ataca un sistema informático como el sistema que es víctima del ataque se encuentran en su territorio, y cuando el sistema informático víctima del ataque se encuentre en su territorio, incluso si el atacante no lo está.

234. Se consideró la posibilidad de incluir una disposición que exija que cada Parte afirme su jurisdicción sobre los delitos relacionados con los satélites registrados en su nombre. Quienes redactaron el Convenio decidieron que esa disposición era innecesaria, ya que las comunicaciones ilícitas que involucren el uso de satélites se originan invariablemente desde tierra y/o serán recibidas en tierra. Por lo tanto, existirá una de las bases para afirmar la jurisdicción de una Parte establecidas en los acápites 1.a) a 1.c) si la transmisión se origina o termina en uno de los lugares especificados en los mismos. Además, en la medida en que el delito que involucre una comunicación vía satélite sea cometido por un nacional de una de las Partes si ningún Estado tiene competencia territorial respecto del mismo, habrá una base para afirmar jurisdicción en virtud del párrafo 1.d). Por último, quienes redactaron el Convenio se preguntaron si el registro es una base adecuada para hacer valer la jurisdicción penal, ya que en muchos casos podría no existir ningún nexo significativo entre el delito cometido y el Estado en que esté registrado un satélite ya que el satélite funciona como un mero conducto de la transmisión.

235. Los acápites b) y c) del párrafo 1 están basados en una variante del principio de territorialidad. Esos acápites requieren que cada Parte afirme su jurisdicción penal respecto de los delitos que se cometan a bordo de un buque que enarbole su pabellón o a bordo de una aeronave matriculada según sus leyes. Esta obligación ya se aplica con carácter general en las leyes de muchos Estados, puesto que los buques y aeronaves a menudo son considerados como una extensión del territorio del Estado. Este tipo de

jurisdicción es útil principalmente cuando el buque o la aeronave no se encuentra en su territorio en el momento en que se comete el delito; como consecuencia de ello, no se podría recurrir al acápite a) del párrafo 1 como base para afirmar su jurisdicción. Si el delito es cometido a bordo de un buque o una aeronave que se encuentra fuera del territorio del Estado de pabellón, de no ser por este requisito podría ocurrir que ningún otro Estado fuera capaz de afirmar su jurisdicción. Además, si se comete un delito a bordo de un buque o una aeronave que esté simplemente atravesando las aguas o el espacio aéreo de otro Estado, este Estado pueden enfrentarse a importantes obstáculos prácticos para afirmar su jurisdicción, por lo que es útil que el Estado donde está registrado el buque o la aeronave puedan también afirmar jurisdicción.

236. El acápite d) del párrafo 1 está basado en el principio de la nacionalidad. La teoría de la nacionalidad es aplicada más frecuentemente por los Estados que se basan en la tradición del derecho civil. Establece que los nacionales de un Estado están obligados a cumplir con las leyes nacionales, incluso cuando se encuentran fuera de su territorio. Conforme a lo dispuesto en el acápite d), si una persona de una determinada nacionalidad comete un delito en el extranjero, la Parte está en la obligación de contar con la capacidad de procesarlo si la conducta constituye también un delito en virtud de la legislación del Estado en el que se cometió el delito o si la conducta tuvo lugar fuera de la jurisdicción territorial de un Estado.

237. El párrafo 2 permite a las Partes formular una reserva respecto de las bases para afirmar jurisdicción establecidas en el párrafo 1, acápites b), c) y d). Sin embargo, no se permite ninguna reserva respecto de la afirmación de la jurisdicción territorial reflejada en el acápite a), o respecto de la obligación de afirmar jurisdicción en los casos contemplados en el principio de *aut dedere aut judicare* (extraditar o juzgar) en virtud del párrafo 3, es decir, cuando una Parte se ha negado a extraditar al presunto delincuente basándose en su nacionalidad y el acusado se encuentre presente en su territorio. La jurisdicción afirmada en base al párrafo 3 es necesaria para asegurar que aquellas Partes que se nieguen a extraditar a un ciudadano tengan en cambio la capacidad jurídica que les permita llevar a cabo las investigaciones y los procedimientos en su territorio, si así lo requiere la Parte que solicitó la extradición de conformidad con los requisitos sobre "extradición" previstos en el Artículo 24, párrafo 6 del presente Convenio.

238. Las bases de la jurisdicción que figuran en el párrafo 1 no son exclusivas. El párrafo 4 de este Artículo permite que las Partes afirmen también otros tipos de jurisdicción penal de conformidad con su derecho interno.

239. En el caso de delitos cometidos mediante el uso de sistemas informáticos, habrá ocasiones en las que más de una Parte tenga jurisdicción sobre todos o algunos de las personas que han perpetrado el delito. Por ejemplo, muchos ataques de virus, fraudes e infracciones de la propiedad

intelectual cometidos mediante el uso de Internet están dirigidos a víctimas radicadas en muchos Estados. Con el fin de evitar la duplicación de esfuerzos, molestias innecesarias a los testigos, o la competencia entre los funcionarios encargados de aplicar las leyes de los Estados involucrados, o para potenciar la eficiencia o la equidad del proceso, las Partes afectadas realizarán consultas con el fin de determinar la jurisdicción apropiada para interponer una acción judicial. En algunos casos, será más eficaz que los Estados interesados elijan un solo lugar para la acción judicial; en otros, puede ser preferible que un Estado procese a algunos participantes, mientras que uno o más Estados se encargan de procesar a los demás. Ambas opciones están permitidas en virtud del presente párrafo. Por último, la obligación de consulta no es absoluta, sino que ha de tener lugar "cuando ello sea oportuno". Así, por ejemplo, si una de las Partes sabe que la consulta no es necesaria (por ej., ha recibido confirmación de que la otra Parte no tiene la intención de tomar medidas), o si una Parte considera que la consulta puede afectar su investigación o procedimiento, puede demorar las consultas, o negarse a efectuar consultas.

Capítulo III - Cooperación internacional

240. El capítulo III contiene una serie de disposiciones relativas a la extradición y asistencia jurídica mutua entre las Partes.

Sección 1 - Principios generales

Título 1 - Principios generales relativos a la cooperación internacional

Principios generales relativos a la cooperación internacional (Artículo 23)

241. El Artículo 23 establece tres principios generales relativos a la cooperación internacional en el marco del Capítulo III.

242. El artículo comienza señalando que las Partes cooperarán entre sí "en la mayor medida posible." Este principio exige que las Partes se brinden una amplia cooperación recíproca, y que reduzcan al mínimo los impedimentos a la circulación fluida y rápida de la información y las pruebas a nivel internacional.

243. El Artículo 23 establece a continuación el alcance general de la obligación de cooperar: la cooperación abarcará todos los delitos penales relacionados con sistemas y datos informáticos (es decir, los delitos comprendidos en el Artículo 14, párrafo 2, acápites a) y b)), y también la obtención de pruebas en formato electrónico de los delitos. Esto quiere decir que los términos del capítulo III son aplicables tanto cuando un delito se

comete utilizando un sistema informático, o cuando un delito común que no se ha cometido mediante el uso de un sistema informático (por ejemplo, un asesinato) involucra pruebas electrónicas. Sin embargo, cabe señalar que los artículos 24 (Extradición), 33 (Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico) y 34 (Asistencia mutua en relación con la interceptación de datos relativos al contenido) permiten que las Partes prevean diferentes modalidades para la aplicación de estas medidas.

244. Por último, la cooperación se llevará a cabo "de conformidad con las disposiciones del presente Capítulo" y "en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca, y de su propio derecho interno". Esta última cláusula establece el principio general de que las disposiciones del Capítulo III no reemplazan las disposiciones de los acuerdos internacionales en materia de asistencia jurídica mutua y extradición, los acuerdos de reciprocidad entre las Partes (que se describen en mayor detalle en la discusión del Artículo 27 *infra*), o las disposiciones pertinentes del derecho interno de cada país en materia de cooperación internacional. Este principio básico está explícitamente reforzado en los artículos 24 (Extradición), 25 (Principios generales relativos a la asistencia mutua), 26 (Información espontánea), 27 (Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables), 28 (Confidencialidad y restricciones de uso), 31 (Asistencia mutua en relación con el acceso a datos almacenados), 33 (Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico) y 34 (Asistencia mutua en relación con la interceptación de datos relativos al contenido).

Título 2 - Principios relativos a la extradición

Extradición (Artículo 24)

245. El párrafo 1 especifica que la obligación de otorgar la extradición se aplica sólo a los delitos definidos de conformidad con los Artículos 2 a 11 del Convenio que sean castigados por la legislación de las dos Partes implicadas con una pena de privación de libertad de una duración máxima de al menos un año, o con una pena más severa. Quienes redactaron el Convenio decidieron especificar una pena mínima porque, en virtud del Convenio, las Partes pueden castigar algunos de esos delitos con un período máximo de privación de libertad relativamente corto (véase por ej., el Artículo 2 (Acceso ilícito) y el Artículo 4 (Ataques a la integridad de los datos). En vista de ello, a la hora de redactar el Convenio no se estimó oportuno exigir que cada uno de los delitos establecidos en los artículos 2 a 11 sean considerados extraditables *per se*. En consecuencia, se llegó a un acuerdo sobre la exigencia general de que un delito pueda dar lugar a extradición si -- como prevé el Artículo 2 del Convenio Europeo de Extradición (STE núm. 24) -- la pena máxima que cabría imponer como castigo del delito que da lugar a la demanda de extradición tuviera una duración de al menos un año de

privación de libertad. La determinación de si un delito puede o no dar lugar a extradición no depende de la sanción impuesta en un caso concreto, sino en cambio del período máximo de privación de libertad que legalmente pudiera ser impuesta por el delito que da lugar a la demanda de extradición.

246. Al mismo tiempo, de acuerdo con el principio general de que la cooperación internacional en virtud del Capítulo III debería estar conforme a lo dispuesto en los instrumentos en vigor entre las Partes, el párrafo 1 también establece que cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, o de un acuerdo basado en legislación uniforme recíproca (véase la descripción de este término en la discusión del Artículo 27 *infra*), se aplicará la pena mínima prevista en dicho tratado o acuerdo. Por ejemplo, muchos tratados de extradición entre países europeos y no europeos establecen que un delito puede dar lugar a extradición sólo si la pena máxima es superior a un año de privación de libertad o si puede aplicarse una pena más severa. En tales casos, los funcionarios encargados de los casos de extradición internacional seguirán aplicando el mínimo normal conforme a lo previsto en sus tratados para determinar si un delito puede dar lugar a extradición. Incluso en el marco del Convenio Europeo de Extradición (STE núm. 24), las reservas pueden especificar una pena mínima distinta para obtener la extradición. Entre las Partes en ese Convenio, cuando una Parte que ha formulado esa reserva solicita la extradición, se aplicará la pena prevista en la reserva para determinar si el delito puede dar lugar a extradición.

247. El párrafo 2 establece que los delitos descritos en el párrafo 1 deberán estar incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes, y que éstas se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir. Esto no significa que la extradición debe ser otorgada en todas las ocasiones en que se reciba una demanda sino más bien que debe existir la posibilidad de conceder la extradición de personas por tales delitos. Conforme a lo dispuesto en el párrafo 5, las Partes pueden establecer otros requisitos para la extradición.

248. En virtud del párrafo 3, cuando una Parte que condicione la extradición a la existencia de un tratado de extradición con la Parte requirente, o al hecho que los tratados existentes no contemplan una demanda formulada respecto de los delitos establecidos con arreglo a este Convenio, podrá tomar el presente Convenio como fundamento jurídico de la extradición, si bien no está obligada a hacerlo.

249. Cuando una Parte que no condiciona la extradición a la existencia de un tratado utiliza una disposición legal general para proceder a la extradición, el párrafo 4 obliga a incluir los delitos mencionados en el párrafo 1 como delitos que pueden dar lugar a extradición entre ambas.

250. El párrafo 5 establece que la Parte a la que se le solicitó la extradición no está en la obligación de concederla si no está convencida de que se han cumplido todas las condiciones previstas en el tratado o en el derecho interno aplicable. Este es otro ejemplo del principio de que la cooperación deberá ajustarse a lo dispuesto en los instrumentos internacionales aplicables en vigor entre las Partes, en los acuerdos de reciprocidad, o en el derecho interno. Por ejemplo, las condiciones y restricciones establecidas en el Convenio Europeo de Extradición (STE núm. 24) y sus Protocolos adicionales (STE núm. 86 y 98) se aplicarán a las Partes contratantes en dichos acuerdos, y la extradición puede ser rechazada en base a ellos (por ejemplo, el Artículo 3 del Convenio Europeo de Extradición dispone que la extradición podrá ser denegada si el delito es considerado de carácter político, o si se considera que la demanda se ha hecho con el fin de procesar o castigar a una persona, entre otras cosas, por motivos raciales o religiosos, o por su nacionalidad u opinión política).

251. El párrafo 6 se aplica el principio *aut dedere aut judicare* (extraditar o procesar). Como muchos Estados rechazan la extradición de sus ciudadanos, los acusados que se encuentran en el territorio de la Parte de la cual tienen la nacionalidad pueden evitar la responsabilidad por un delito cometido en otra Parte a menos que las autoridades locales estén obligadas a tomar medidas. En virtud del párrafo 6, si la otra Parte ha solicitado la extradición del acusado, y la extradición ha sido rechazada en razón de que el acusado tiene la nacionalidad de la Parte requerida, ésta deberá, a petición de la Parte requirente, someter el asunto a sus autoridades competentes a efectos de la acción penal pertinente. Si la Parte cuya petición de extradición ha sido rechazada no solicita que se lleve a cabo una investigación y una acción judicial a nivel local, la Parte requerida no tiene la obligación de iniciar las acciones. Por otra parte, si no se ha presentado ningún pedido de extradición, o si la extradición ha sido denegada por motivos que no sean el de la nacionalidad, este párrafo no impone ninguna obligación a la Parte requerida para que inicie una acción penal a nivel nacional. Además, el párrafo 6 dispone que la investigación local y la acción judicial se lleven a cabo con diligencia; deben ser tratados con la misma seriedad "que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte". Esta informará a la Parte requirente de los resultados de su investigación y sus actuaciones.

252. A fin de que cada Parte sepa a quién deben estar dirigidas sus demandas de detención provisional o de extradición, el párrafo 7 requiere que las Partes comuniquen al Secretario General del Consejo de Europa el nombre y la dirección de cada autoridad responsable del envío o la recepción de las demandas de extradición o de detención provisional en ausencia de tratado. Esta disposición se ha limitado a situaciones en las cuales no existe un tratado de extradición vigente entre las Partes involucradas ya que si un tratado de extradición bilateral o multilateral está en vigor entre las Partes (por ejemplo, el STE núm. 24), las Partes sabrán a quién han de dirigirse los pedidos de extradición o de arresto provisional, sin la necesidad de un

requisito de registro. La comunicación al Secretario General debe hacerse en el momento de la firma o cuando la Parte deposite el instrumento de ratificación, aceptación, aprobación o adhesión del presente Convenio. Cabe señalar que la designación de una autoridad no excluye la posibilidad de utilizar la vía diplomática.

Título 3 - Principios generales relativos a la asistencia mutua

Principios generales relativos a la asistencia mutua (Artículo 25)

253. Los principios generales que rigen la obligación de prestar asistencia mutua se establecen en el párrafo 1. Las Partes "se prestarán toda la ayuda mutua posible". Así, al igual que en el Artículo 23 ("Principios generales relativos a la cooperación internacional"), la asistencia mutua ha de ser, en principio, amplia y los obstáculos a la misma deberán estar estrictamente limitados. En segundo lugar, al igual que en el Artículo 23, la obligación de cooperar se aplica en principio tanto a los delitos penales relacionados con sistemas y datos informáticos (es decir, los delitos contemplados en el Artículo 14, párrafo 2, acápites a) y b)), como a la obtención de pruebas en formato electrónico de un delito penal. Se acordó imponer la obligación de cooperar respecto de esta amplia clase de delitos porque existe la misma necesidad de contar con mejores mecanismos de cooperación internacional respecto de ambas categorías. Sin embargo, los Artículos 34 y 35 permiten a las Partes establecer un alcance diferente para la aplicación de estas medidas.

254. Otras disposiciones de este Capítulo aclararán que la obligación de prestar asistencia mutua se lleva a cabo en general de conformidad con los términos de los tratados, las leyes y los acuerdos de asistencia legal aplicables. En virtud del párrafo 2, cada Parte tiene la obligación de tener una base jurídica para llevar a cabo las formas específicas de cooperación enunciadas en el resto del Capítulo, si sus tratados, leyes y acuerdos no contienen ya tales disposiciones. La disponibilidad de dichos mecanismos, en particular los contenidos en los Artículos 29 a 35 (Disposiciones específicas - Títulos 1, 2 y 3), es vital para una eficaz cooperación en los asuntos penales relacionados con la informática.

255. Algunas Partes no requerirán que esté legislada su implementación para poder aplicar las disposiciones contempladas en el párrafo 2, ya que se considera que las disposiciones de los tratados internacionales que establecen regímenes de asistencia mutua detallada son, por naturaleza, directamente aplicables (*self-executing*). Se espera que las Partes puedan considerar estas disposiciones directamente aplicables, o que en virtud de la legislación vigente sobre asistencia mutua tengan suficiente flexibilidad para poner en práctica las medidas de asistencia mutua establecidas en este Capítulo, o que puedan aprobar rápidamente cualquier legislación necesaria para ello.

256. Los datos informáticos son muy volátiles. Al pulsar unas pocas teclas o mediante la operación de programas automáticos, estos pueden ser eliminados, haciendo imposible seguir la pista de un delito hasta su autor o destruyendo pruebas esenciales de su culpabilidad. Algunas formas de datos informáticos están almacenados sólo por cortos períodos de tiempo antes de ser eliminados. En otros casos, se puede causar un daño significativo a personas o bienes si las pruebas no se reúnen con rapidez. En esos casos urgentes, no sólo el pedido, sino también la respuesta deben hacerse de una manera acelerada. El objetivo del párrafo 3 es, por lo tanto, facilitar la aceleración del proceso de obtención de asistencia mutua de manera tal que la información o las pruebas esenciales no se pierdan debido a que han sido eliminadas antes de que pudiera prepararse, transmitirse y dar respuesta al pedido de asistencia. El párrafo 3 lo hace 1) facultando a las Partes a formular demandas urgentes de cooperación a través de medios de comunicación expeditivos, en lugar de a través de la tradicional y mucho más lenta de documentos escritos y sellados enviados por valijas diplomática o sistemas de entrega de correspondencia, y 2) exigiendo que la Parte requerida utilice medios acelerados para responder a las demandas en tales circunstancias. Cada Parte deberá tener la capacidad de aplicar esta medida si sus tratados, leyes y acuerdos de asistencia mutua no lo establecen previamente. La mención del fax y del correo electrónico se hacen solo a título indicativo; se puede utilizar cualquier otro medio de comunicaciones rápidos, si fuera apropiado en las circunstancias particulares en que se esté. A medida que avanza la tecnología, se desarrollarán otros medios de comunicación más expeditivos que podrán ser utilizados para solicitar la asistencia mutua. Con respecto al requerimiento de autenticidad y seguridad contenido en el párrafo, las Partes pueden decidir entre ellas la manera de asegurar la autenticidad de las comunicaciones y si existe la necesidad de establecer protecciones especiales de seguridad (incluido el cifrado) que puede ser necesarias en casos especialmente sensibles . Por último, el párrafo también permite que la Parte requerida exija una confirmación oficial enviada a través de los canales tradicionales o, si lo prefiere, a través de la vía rápida.

257. El párrafo 4 establece el principio de que la asistencia mutua está sujeto a los términos de los tratados de asistencia mutua aplicables y en el derecho interno de la Parte requerida. Estos regímenes establecen salvaguardias para los derechos de las personas que se encuentran en el territorio de la Parte requerida, que puede ser objeto de una demanda de asistencia mutua. Por ejemplo, una medida intrusiva, tal como la de registro y confiscación, no se lleva a cabo en nombre de la Parte requirente, a menos que se hayan satisfecho los requisitos fundamentales para dicha medida aplicables en un caso nacional de la Parte requerida. Las Partes pueden también garantizar la protección de los derechos de las personas en relación con los bienes incautados en virtud de la asistencia mutua.

258. Sin embargo, el párrafo 4 no se aplica "salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo". Esta cláusula está destinada a señalar que el Convenio contiene varias excepciones significativas al principio general. La primera de dichas excepciones ha sido vista en el párrafo 3 de este artículo; la misma obliga a cada Parte a establecer las formas de cooperación establecidas en los restantes artículos del Capítulo (tales como la conservación, la obtención de datos en tiempo real, el registro y confiscación, y el mantenimiento de una red las 24 horas los 7 días de la semana), sin tener en cuenta si sus tratados de asistencia jurídica mutua, sus acuerdos equivalentes o las leyes sobre asistencia mutua establecen actualmente dichas medidas. Otra excepción se encuentra en el Artículo 27, que siempre ha de aplicarse a la ejecución de los pedidos en lugar del derecho interno de la Parte requerida que rigen en materia de cooperación internacional ante la ausencia de un tratado de asistencia mutua o acuerdo equivalente entre ambas Partes. El Artículo 27 establece un sistema de condiciones y motivos de denegación. Otra excepción, específicamente prevista en este párrafo, es que la cooperación no puede ser denegada, al menos en lo que se refiere a los delitos tipificados en los artículos 2 a 11 del Convenio, en razón de que la Parte requerida considera que la demanda implican un delito "penal". Por último, el Artículo 29 es una excepción, ya que establece que la conservación no puede ser denegada por razones de doble tipificación penal, aunque se establece la posibilidad de formular una reserva al respecto.

259. El párrafo 5 es esencialmente una definición de lo que se entiende por doble tipificación penal a los fines de la asistencia mutua conforme a este Capítulo. Cuando la Parte requerida se permite exigir la doble tipificación penal como condición para la prestación de asistencia (por ej., cuando la Parte requerida se ha reservado el derecho de exigir la doble tipificación penal con respecto a la conservación de los datos en virtud del párrafo 4 del Artículo 29 ("Conservación rápida de datos informáticos almacenados"), se considerará que existe doble tipificación constitutiva del delito por el cual se pide la asistencia es también un delito conforme a las leyes de la Parte requerida, incluso si sus leyes ubican dicho delito dentro de una categoría diferente de delitos o si utilizan una terminología diferente para denominar el delito. Esta disposición fue considerada necesaria con el fin de garantizar que las Partes a las que se les pidió la asistencia no adopten una prueba demasiado rígida al aplicar la doble tipificación penal. En vista de las diferencias que existen entre los sistemas jurídicos de cada país, es lógico que existan variaciones respecto de la terminología y la clasificación de las conductas delictivas. Si la conducta constituye una violación penal en virtud de ambos sistemas, dichas diferencias técnicas no deberían impedir la asistencia. Más bien, en aquellas cuestiones en las cuales es aplicable la norma de la doble tipificación penal, esta debería aplicarse de manera flexible que facilite la concesión de la ayuda.

Información espontánea (Artículo 26)

260. Este artículo se deriva de las disposiciones incluidas en anteriores instrumentos del Consejo de Europa, tales como el artículo 10 del *Convenio* sobre el *blanqueo*, investigación, la confiscación y el decomiso del producto del delito (*STE núm. 141*) y el artículo 28 del *Convenio de Derecho penal* contra la corrupción del *Consejo de Europa* (STE núm. 173). Cada vez más frecuentemente, una Parte posee información valiosa que cree que puede ayudar a la otra Parte en una investigación o procedimiento penal, y que la Parte que realiza la investigación o procedimiento no sabe que existe. En tales casos, no se efectuará ningún pedido de asistencia mutua. El párrafo 1 faculta al Estado en posesión de la información a transmitirla a otro Estado sin que medie una demanda previa. La disposición se considera útil, ya que, en virtud de las leyes de algunos Estados, es necesario un permiso positivo de una autoridad judicial para prestar asistencia en ausencia de una demanda. Ninguna Parte está obligada a enviar espontáneamente información a otra Parte; puede ejercer su facultad de discreción a la luz de las circunstancias del caso. Además, la revelación espontánea de información no se opone a que la Parte que revela la misma, si tiene jurisdicción, investigar o entablar procedimientos en relación con los hechos revelados.

261. El párrafo 2 aborda el hecho de que en determinadas circunstancias, una Parte sólo transmitirá información de manera espontánea, si la información sensible ha de ser mantenida en forma confidencial y si se pueden imponer otras condiciones sobre el uso de la información. En particular, la confidencialidad será una consideración importante en aquellos casos en que pueden estar en peligro intereses importantes del Estado que suministra la información si la información se hiciera pública, por ej., cuando existe la necesidad de proteger la identidad de un medio empleado para reunir información o el hecho de que se esté investigando a un grupo delictivo. Si una investigación avanzada revela que la Parte receptora no puede cumplir con una condición exigida por la Parte emisora (por ejemplo, cuando no puede cumplir con una condición de confidencialidad, porque la información es necesaria como prueba en un juicio público), la Parte receptora deberá advertir a la Parte emisora, la que entonces tiene la opción de no proporcionar la información. Sin embargo, si la Parte receptora acepta la condición, debe cumplirla. Se prevé que las condiciones impuestas en virtud de este artículo han de ser coherentes con las que podrían ser impuestas por la Parte emisora de conformidad con una solicitud de asistencia mutua de la Parte receptora.

Título 4 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables (Artículo 27)

262. El Artículo 27 obliga a las Partes a aplicar determinados procedimientos y condiciones de asistencia mutua cuando no existen tratados o acuerdos de asistencia mutua en base a una legislación uniforme o recíproca vigente entre las Partes requirentes de asistencia mutua y las Partes requeridas. El artículo refuerza de esta forma el principio general de que la asistencia mutua debe llevarse a cabo mediante la aplicación de los tratados pertinentes de asistencia mutua y otros acuerdos similares. Quienes redactaron el Convenio rechazaron la creación de un régimen general separado de asistencia mutua en el presente Convenio que se aplicaría en lugar de otros instrumentos y acuerdos aplicables, acordando en cambio que sería más práctico basarse en los regímenes de los tratados de asistencia mutua existentes como una cuestión general, permitiendo así que quienes practiquen la asistencia mutua utilicen instrumentos y acuerdos con los que estén más familiarizados y evitando la confusión que podría resultar del establecimiento de regímenes que compitan entre sí. Como se señaló anteriormente, sólo con respecto a los mecanismos que son particularmente necesarios para una rápida cooperación eficaz en los asuntos penales relacionados con la informática, tales como los contenidos en los Artículos 29 a 35 (Disposiciones específicas - Títulos 1, 2 y 3), se requiere a que cada Parte establezca un fundamento jurídico que permita el llevar a cabo tales formas de cooperación en caso de que sus tratados, acuerdos y leyes actuales sobre asistencia mutua aún no lo hagan.

263. Por consiguiente, la mayoría de las formas de asistencia mutua conforme a este Capítulo se seguirán llevando a cabo de conformidad con el Convenio Europeo de Asistencia Judicial en Materia Penal (STE núm. 30) y su Protocolo (STE núm. 99) entre las Partes en esos instrumentos. Alternativamente, las Partes en este Convenio que tengan acuerdos de asistencia mutua bilaterales vigentes entre sí, u otros acuerdos multilaterales sobre asistencia mutua en asuntos penales (por ej., entre los Estados miembros de la Unión Europea), deberán seguir aplicando sus términos, complementados por los mecanismos específicos para los delitos informáticos o los delitos relacionados con la informática descritos en el resto del capítulo III, salvo que acuerden aplicar alguna o todas las disposiciones del presente Artículo, en lugar de los mismos. La asistencia mutua también puede basarse en acuerdos convenidos en base a una legislación uniforme y recíproca, tal como el sistema de cooperación desarrollado entre los países nórdicos, que también es admitido por el Convenio Europeo de Asistencia Judicial en Materia Penal (Artículo 25, párrafo 4), y entre los miembros de la Commonwealth. Por último, la referencia a los tratados o a los acuerdos de asistencia mutua en base a una legislación uniforme o recíproca, no se limita a aquellos instrumentos vigentes al momento de la entrada en vigor del presente Convenio, pero abarca también los instrumentos que pueden adoptarse en el futuro.

264. El Artículo 27 (procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables), párrafos 2 a 10, establece una serie de normas para la prestación de asistencia mutua en la

ausencia de un tratado de asistencia mutua o de un acuerdo sobre la base de una legislación uniforme o recíproca, incluyendo el establecimiento de autoridades centrales, la imposición de las condiciones, motivos y procedimientos en los casos de aplazamiento o rechazo, la confidencialidad de las solicitudes y de las comunicaciones directas. Con respecto a dichas cuestiones expresamente contemplados en la ausencia de un convenio o acuerdo de asistencia mutua en base a una legislación uniforme o recíproca, se aplicarán las disposiciones del presente artículo en lugar de otras leyes nacionales aplicables en materia de asistencia mutua. Al mismo tiempo, el Artículo 27 no establece normas para otras cuestiones que suelen abordarse en la legislación nacional respecto de la asistencia mutua internacional. Por ejemplo, no existe ninguna disposición relativa a la forma y el contenido de las solicitudes, la manera de tomar declaraciones a los testigos en la Parte requerida o la Parte requirente, la provisión de registros oficiales o comerciales, la transferencia de testigos bajo custodia, o la asistencia en caso de que deban efectuarse decomisos. Con respecto a estas cuestiones, el Artículo 25, párrafo 4, establece que a falta de una disposición específica en este Capítulo, el derecho de la Parte requerida deberá regir las modalidades específicas respecto de proveer ese tipo de asistencia.

265. El párrafo 2 requiere el establecimiento de una autoridad o autoridades centrales responsables de enviar y responder a las solicitudes de asistencia. La institución de las autoridades centrales es una característica común de los instrumentos modernos en materia de asistencia mutua sobre asuntos penales, y es especialmente útil para asegurar el tipo de reacción rápida que es tan útil en la lucha contra los delitos informáticos y los delitos relacionados con la informática. Inicialmente, la transmisión directa entre dichas autoridades es más rápida y eficiente que la transmisión realizada a través de los canales diplomáticos. Además, el establecimiento de una autoridad central activa cumple una importante función en garantizar que tanto las solicitudes recibidas como las emitidas se tramitaron diligentemente, que se proporciona asesoramiento a las autoridades extranjeras a cargo de hacer cumplir la ley respecto de la mejor manera de satisfacer los requisitos legales en la Parte requerida, y que las solicitudes particularmente urgentes o sensibles son tratadas adecuadamente.

266. Se alienta a las Partes como una cuestión de eficiencia a que designen una única autoridad central respecto de la asistencia mutua; por lo general, sería más eficiente que la autoridad designada para tal fin en virtud de un tratado de asistencia mutua de la Parte, o en virtud del derecho interno, fuera también la autoridad central cuando sea aplicable este artículo. Sin embargo, las Partes tienen flexibilidad para designar más de una autoridad central cuando esto fuere pertinente en virtud de sus respectivos sistemas de asistencia mutua. Cuando se establezca más de una autoridad central, la Parte que ha hecho esto, debería asegurar que cada autoridad interprete las disposiciones del Convenio de la misma manera, y que todas las solicitudes, tanto las recibidas como las emitidas, son tratadas con rapidez y eficacia. Cada Parte ha de comunicar al Secretario General del Consejo de Europa los

nombres y domicilios (incluidos la dirección de correo electrónico y el número de fax) de la autoridad o autoridades designadas para recibir y responder a las solicitudes de asistencia mutua en virtud del presente artículo, y las Partes están obligadas a garantizar que esa información se mantiene al día.

267. Un objetivo importante de un Estado que solicita asistencia mutua a menudo es asegurar que se cumplen las leyes nacionales que rigen la admisibilidad de las pruebas, y que por consiguiente las pruebas se pueden utilizar ante sus tribunales. Para asegurarse de que pueden cumplirse tales requisitos respecto de las pruebas, el párrafo 3 obliga a la Parte requerida que de curso a las solicitudes de conformidad con los procedimientos especificados por la Parte requirente, a menos que ello fuere incompatible con su legislación. Se hace hincapié en que este párrafo se refiere únicamente a la obligación de respetar los requisitos técnicos de procedimiento, no las salvaguardias procesales fundamentales. Así, por ejemplo, la Parte requirente no puede exigir a la Parte requerida que proceda a un registro y confiscación si no se cumplen los requisitos fundamentales para que se tome esta medida conforme a las leyes de esta última. A la luz de la naturaleza limitada de la obligación, se acordó que el mero hecho de que el sistema jurídico de la Parte requerida no contemple ese procedimiento no es un motivo suficiente para denegar la aplicación del procedimiento solicitado por la Parte requirente; en cambio, el procedimiento debe ser incompatible con los principios jurídicos de la Parte requerida. Por ejemplo, en virtud de la legislación de la Parte requirente, un requisito procesal puede ser que la declaración de un testigo debe hacerse bajo juramento. Incluso si la Parte requerida no contempla este requisito en su derecho interno, deberá acceder a la solicitud de la Parte requirente.

268. El párrafo 4 prevé la posibilidad de rechazar las solicitudes de solicitudes de asistencia mutua formuladas con arreglo a este artículo. La asistencia podrá denegarse por los motivos previstos en el Artículo 25, párrafo 4 (es decir, los motivos previstos en la legislación de la Parte requerida), incluyendo perjuicio de la soberanía del Estado, a la seguridad, al orden público o a otros intereses fundamentales, y cuando el delito es considerado por la Parte requerida como un delito político o un delito relacionado con un delito político. A fin de promover el principio fundamental de proporcionar la mayor cooperación posible (véanse los Artículos 23 y 25), los motivos establecidos por la Parte requerida para rechazar la solicitud deberían ser pocos y se deberían ejercer con moderación. No deberían ser tan amplios como para crear el potencial para denegar categóricamente la asistencia, ni estar sujetos a condiciones onerosas, ni incluir amplias categorías de pruebas o de información.

269. En consonancia con este enfoque, se entiende que, aparte de los motivos establecidos en el Artículo 28, la denegación de asistencia por motivos de protección de los datos sólo podrá invocarse en casos excepcionales. Tal situación podría producirse si, al valorar los intereses importantes en juego en el caso particular (por un lado, los intereses

públicos, incluida la buena administración de justicia y, por otro lado, los intereses del respeto de la vida privada), la entrega de los datos concretos solicitados por la Parte requirente pudiese crear dificultades tan fundamentales que pudieran llevar a la Parte requerida a considerar su denegación en razón de intereses esenciales. Por consiguiente, queda excluida una aplicación amplia, categórica o sistemática de los principios de protección de los datos con el fin de rechazar la cooperación. Así, el hecho de que las Partes interesadas tengan diferentes sistemas de protección de la privacidad de los datos (por ejemplo, que la Parte requirente no tenga el equivalente de una autoridad especializada en la protección de los datos) o que tengan métodos distintos de protección de los datos personales (como el que la Parte requirente utiliza otros medios diferentes del proceso de borrado para proteger la privacidad o la exactitud de los datos personales recibidos por las autoridades competentes), no constituye como tal motivo para denegar asistencia. Antes de invocar "intereses esenciales", como base para rechazar la cooperación, la Parte requerida debería en su lugar tratar de fijar condiciones que pudieran permitir la transferencia de los datos. (véase el Artículo 27, párrafo 6 y el párrafo 271 del presente informe).

270. El párrafo 5 permite que la Parte requerida posponga el brindar asistencia, en lugar de denegarla, cuando tomar medidas inmediatas respecto de la solicitud podría ser perjudicial para las investigaciones y procedimientos que se lleven a cabo en territorio de la Parte requerida. Por ejemplo, cuando la Parte requirente ha tratado de obtener pruebas o el testimonio de testigos con el fin de realizar una investigación o para un juicio, y las mismas pruebas o testimonios son necesarios para ser utilizados en un juicio que esté a punto de comenzar en la Parte requerida, ésta tendría una justificación para posponer la prestación de asistencia.

271. El párrafo 6 establece que, cuando la asistencia solicitada fuera denegada o pospuesta por algún otro motivo, la Parte requerida puede en cambio proveer dicha asistencia sujeta a condiciones. Si no se puede llegar a un acuerdo con la otra Parte respecto de las condiciones, la Parte requerida puede modificarlas o puede ejercer su derecho a denegar o posponer la asistencia. Dado que la Parte requerida tiene la obligación de proporcionar el mayor nivel de asistencia posible, se acordó que tanto los motivos de denegación como la fijación de condiciones deberían ejercerse con moderación.

272. El párrafo 7 obliga a la Parte requerida a mantener informada a la Parte requirente acerca del resultado de la solicitud, y requiere que se expliquen las razones en caso de una negativa o una postergación de la asistencia. Las razones que se aduzcan pueden, entre otras cosas, ayudar a la Parte requirente a cómo ha interpretado la Parte requerida las disposiciones del presente artículo, establecer una base para realizar consultas, a fin de mejorar la eficiencia futura respecto de la asistencia mutua, y proporcionar a la Parte requirente información objetiva previamente desconocida acerca de la disponibilidad o la condición de los testigos o las pruebas.

273. Hay veces en que una Parte formula una solicitud de asistencia respecto de un asunto particularmente delicado, o de un caso que podría tener consecuencias desastrosas si los hechos que fundamentan la solicitud fueran hechos públicos prematuramente. En consecuencia, el párrafo 8 permite que la Parte requirente pida que los hecho y el contenido de la solicitud sean mantenidos en forma confidencial. Sin embargo, la confidencialidad no puede requerirse hasta el extremo de socavar la capacidad de la Parte requerida para obtener las pruebas o la información solicitada, por ejemplo, cuando la información tenga que ser revelada a fin de obtener una orden judicial necesaria para poder brindar la asistencia, o cuando sea necesario informar a las personas que poseen las pruebas respecto de la solicitud de asistencia a fin de poder llevarlo a cabo con éxito. Si la Parte requerida no puede cumplir con el pedido de confidencialidad, deberá notificar a la Parte requirente, la cual tiene entonces la opción de retirar o modificar su petición.

274. Las autoridades centrales designadas de conformidad con el párrafo 2 deberán comunicarse directamente entre sí. Sin embargo, en un caso urgente, las solicitudes de asistencia mutua pueden ser enviadas directamente por los jueces y fiscales de la Parte requirente a los jueces y fiscales de la Parte requerida. El juez o el fiscal que siga este procedimiento debe también dirigir una copia de la solicitud efectuada a su propia autoridad central para que sea transmitida a la autoridad central de la Parte requerida. Bajo el acápite b), las solicitudes pueden canalizarse a través de INTERPOL. Las autoridades de la Parte requerida que recibe una petición que cae fuera de su ámbito de competencia tienen, conforme al acápite c), una doble obligación. En primer lugar, debe transferir la solicitud a la autoridad competente de la Parte requerida. En segundo lugar, deben informar a las autoridades de la Parte requirente de la transferencia realizada. Bajo el acápite d), las solicitudes podrán transmitirse también directamente, sin la intervención de las autoridades centrales, incluso si no son urgentes, siempre y cuando la autoridad de la Parte requerida pueda cumplir con el pedido sin hacer uso de medidas coercitivas. Por último, el acápite e) permite a una Parte informar a las demás, a través del Secretario General del Consejo de Europa, que, por razones de eficacia, las comunicaciones directas han de dirigirse a la autoridad central.

Confidencialidad y restricciones de uso (Artículo 28)

275. Esta disposición establece expresamente limitaciones del uso de la información o los materiales, a fin de posibilitar a la Parte requerida, en los casos en que dicha información o materiales sean particularmente sensibles, asegurar que su uso esté limitado al motivo por el cual se concedió la asistencia, o asegurar que sólo se divulgará ante los funcionarios encargados de hacer cumplir las leyes de la Parte requirente. Estas restricciones proporcionan salvaguardias que están disponibles, entre otras cosas, con el fin de proteger los datos.

276. Como en el caso del Artículo 27, el Artículo 28 sólo se aplica cuando no existe un tratado de asistencia mutua, o un acuerdo en base a una legislación uniforme y recíproca, vigentes entre las Partes. Cuando un tratado o acuerdo de ese tipo esté vigente, se aplicarán sus disposiciones respecto de la confidencialidad y las limitaciones de uso en lugar de las disposiciones de este Artículo, a menos que las mismas Partes acuerden lo contrario. Esto evita la superposición con los tratados de asistencia mutua bilaterales y multilaterales existentes y con otros acuerdos similares, permitiendo que quienes pongan en práctica los mismos sigan operando bajo el régimen normal bien conocido en lugar de tratar de aplicar dos instrumentos distintos y posiblemente contradictorios.

277. El párrafo 2 permite a la Parte requerida, al responder a una solicitud de asistencia mutua, imponer dos tipos de condiciones. En primer lugar, podrá solicitar que la información o material proporcionado sea mantenido en forma confidencial cuando la solicitud no pudiera ser cumplida ante la falta de tal condición, como cuando se trata de la identidad de un informante confidencial. No es apropiado exigir absoluta confidencialidad en los casos en que la Parte requerida tiene la obligación de prestar la asistencia solicitada, ya que ello, en muchos casos, coartaría la capacidad de la Parte requirente para investigar o juzgar con éxito el delito, por ej., utilizando las pruebas en un juicio público (incluidos los procedimientos obligatorios para la presentación de pruebas).

278. En segundo lugar, la Parte requerida podrá hacer entrega de la información o material con la condición de que no sea utilizada para otras investigaciones o procedimientos distintos de los indicados en la solicitud. Para que esta condición se aplique, debe ser invocada expresamente por la Parte requerida; de lo contrario, no existe tal limitación de uso para la Parte requirente. En los casos en que se invoque, esta condición asegurará que la información y el material sólo pueden utilizarse para los fines previstos en la solicitud, lo que excluye el uso del material para otros fines sin el consentimiento de la Parte requerida. Los negociadores reconocieron dos excepciones a la capacidad de limitar el uso, que están implícitas en los términos del párrafo. En primer lugar, en virtud de los principios jurídicos fundamentales de muchos Estados, si el material proporcionado es una prueba exculpatoria para un acusado, se debe poner en conocimiento de la defensa o a la autoridad judicial. Además, la mayoría de los materiales proporcionados en virtud de los regímenes de asistencia mutua está destinado al uso en el juicio, normalmente un juicio público (incluidos los procedimientos obligatorios para la presentación de pruebas). Una vez revelado el material, éste pasa a ser de dominio público. En estos casos, no es posible asegurar la confidencialidad respecto de la investigación o el procedimiento para el cual se solicitó la asistencia mutua.

279. El párrafo 3 establece que si la Parte a la cual se transmite la información no puede cumplir con la condición impuesta deberá notificar a la

Parte emisora, la que entonces tiene la opción de no proveer la información. Sin embargo, si la Parte receptora está de acuerdo con la condición deberá cumplirla.

280. El párrafo 4 establece que puede ser necesario pedir a la Parte requirente que explique el uso dado a la información o material que ha recibido con arreglo a las condiciones descritas en el párrafo 2, a fin de que la Parte requerida pueda determinar si tal condición se ha cumplido. Se acordó que la Parte requerida no puede pedir un control demasiado gravoso, por ej., de cada una de las veces que se ha accedido al material o a la información suministrada.

Sección 2 – Disposiciones específicas

281. La finalidad de la presente sección es establecer mecanismos específicos a fin de adoptar medidas eficaces y concertadas a nivel internacional en los casos que involucren delitos informáticos y pruebas que estén en formato electrónico.

Título 1 - Asistencia mutua en materia de medidas provisionales

Conservación rápida de datos informáticos almacenados (Artículo 29)

282. Este artículo establece un mecanismo a nivel internacional equivalente al prevista en el Artículo 16 para su uso a nivel nacional. El párrafo 1 de este Artículo autoriza a una Parte a hacer una solicitud (y el párrafo 3 establece que cada Parte debe tener la capacidad legal para obtener) la conservación rápida de datos almacenados en el territorio de la Parte requerida por medio de un sistema informático, con el fin de que los datos no sean alterados, retirados o eliminados durante el período de tiempo necesario para preparar, transmitir y ejecutar una solicitud de asistencia mutua para obtener los datos. La conservación es una medida limitada y provisional, concebida para ser aplicada mucho más rápidamente que la ejecución de una solicitud tradicional de asistencia mutua. Como ya se ha indicado previamente, los datos informáticos son muy volátiles. Con unas pocas pulsaciones, o mediante la operación de programas automáticos, pueden ser eliminados, alterados o trasladados, lo que hace imposible seguir la pista de un delito hasta su autor o destruyendo pruebas esenciales de su culpabilidad. Algunas formas de datos informáticos están almacenados sólo por cortos períodos de tiempo antes de ser eliminados. Por ello, se acordó que era necesario contar con un mecanismo para asegurar la disponibilidad de dichos datos, que dependían del proceso mucho más largo y complicado de ejecutar una solicitud formal de asistencia mutua, lo que puede tomar semanas o meses.

283. Si bien es mucho más rápida que la práctica convencional de asistencia mutua, esta medida es al mismo tiempo menos intrusiva. Los funcionarios

encargados de la asistencia mutua de la Parte requerida no están obligados a obtener la posesión de los datos de quien los custodia. El procedimiento preferido es que la Parte requerida asegure que el custodio de los datos (con frecuencia, un proveedor de servicios u otro tercero) preservará (es decir, no eliminará) los datos hasta que se lleve a cabo el proceso que requiere que los mismos sean entregado a los agentes del orden en una etapa posterior. Este procedimiento tiene la ventaja de ser rápido y de proteger la intimidad de la persona a la que corresponden los datos, ya que éstos no serán revelados ni examinados por ningún funcionario gubernamental hasta que se cumplan los criterios estipulados para permitir la revelación plena de los mismos conforme a los regímenes normales de asistencia mutua habituales. Al mismo tiempo, la Parte requerida puede utilizar otros procedimientos para asegurar la conservación rápida de los datos, incluida la emisión acelerada y la ejecución de una orden de suministrar información o de una orden de registro y confiscación de los datos. El principal requisito es contar con un proceso sumamente rápido para evitar que los datos se pierdan irreparablemente.

284. El párrafo 2 establece el contenido de una solicitud de conservación con arreglo a lo dispuesto en este artículo. Teniendo en cuenta que se trata de una medida provisional y que la petición tendrá que ser preparada y transmitida rápidamente, la información suministrada será sumaria e incluirá sólo la información mínima necesaria para permitir la conservación de los datos. Además de especificar la autoridad que solicita la conservación y el delito por el cual se solicita la medida, la solicitud debe incluir una síntesis de los hechos, información suficiente para identificar los datos que han de preservarse y su ubicación, y demostrar que los datos son pertinentes para la investigación o el juicio relacionado con el delito en cuestión y que dicha conservación es necesaria. Por último, la Parte requirente debe comprometerse a presentar posteriormente una solicitud de asistencia mutua para poder obtener la presentación de los datos.

285. El párrafo 3 establece el principio de que no se exigirá como condición la doble tipificación penal para la conservación de los datos. En general, la aplicación del principio de doble tipificación penal es contraproducente en el contexto de la conservación de los datos. En primer lugar, como una cuestión de la práctica moderna respecto de la asistencia mutua, existe la tendencia a eliminar el requisito de la doble tipificación penal para todas las medidas procesales excepto las más intrusivas, tales como el registro y confiscación y la interceptación. Sin embargo, tal como fue prevista por quienes redactaron el Convenio, la conservación no es particularmente intrusiva, ya que el custodio simplemente conserva la posesión de los datos que están legalmente en su poder, y los datos no son revelados o examinados por funcionarios de la Parte requerida hasta después de la ejecución de una solicitud formal de asistencia mutua en que se solicite la divulgación de los datos. En segundo lugar, como cuestión práctica, a menudo lleva mucho tiempo proporcionar las aclaraciones necesarias para establecer de manera concluyente la existencia de la doble tipificación penal, y los datos podrían

ser borrados, eliminados o alterados en el ínterin. Por ejemplo, en las primeras etapas de una investigación, la Parte requirente puede tener conocimiento de que se produjo una intrusión en un ordenador ubicado en su territorio, pero puede no comprender bien hasta mucho más tarde la naturaleza y magnitud del daño. Si la Parte requerida se demora en la conservación de los datos relativos al tráfico que pudieran servir para llegar hasta el origen de la intrusión, respecto de la cual está pendiente determinar la doble tipificación penal, los datos esenciales a menudo podrían ser eliminados de manera habitual por los proveedores de servicios que solo los conservan algunas horas o días después de efectuada la transmisión. Incluso si posteriormente la Parte requirente pudiera establecer la doble tipificación penal, los datos cruciales relativos al tráfico podrían no ser recuperados y el autor del delito nunca sería identificado.

286. Por consiguiente, la regla general es que las Partes deben prescindir de cualquier requisito de doble tipificación del delito a los fines de la conservación. Sin embargo, está disponible una reserva limitada en virtud del párrafo 4. Si una Parte exige la doble tipificación penal como condición para responder a una solicitud de asistencia mutua para el suministro de los datos, y si tiene motivos para creer que, en el momento de la divulgación, no se cumplirá el principio de la doble tipificación penal, puede reservarse el derecho de exigir la doble tipificación penal como condición previa para efectuar la conservación de los datos. Con respecto a los delitos establecidos conforme a los Artículos 2 a 11, se da por supuesto que el requisito de doble incriminación penal se cumple automáticamente entre las Partes, sujeta a cualquier reserva que las Partes pudieran haber hecho respecto de estos delitos en los casos permitidos por el Convenio. En consecuencia, las Partes pueden imponer esta obligación sólo en relación con otros delitos que no estén definidos en el Convenio.

287. De lo contrario, en virtud del párrafo 5, la Parte requerida sólo podrá rechazar una solicitud de conservación de datos cuando su ejecución perjudicaría su soberanía, la seguridad, el orden público u otros intereses fundamentales, o cuando se considere que el delito es un delito político o un delito relacionado con un delito político. Debido al carácter central de esta medida para una investigación o un juicio eficaz en relación a un delito informático o a un delito relacionado con la informática, se acordó que se excluye la posibilidad de considerar cualquier otro fundamento para rechazar una solicitud de conservación.

288. A veces, la Parte requerida puede darse cuenta de que es probable que el custodio de los datos puede tomar medidas que amenazan la confidencialidad, o causarían prejuicio a la investigación de la Parte (requirente por ejemplo, cuando los datos que se desea conservan están en poder de un proveedor de servicios controlado por un grupo criminal, o por quien es objeto de la investigación misma). En tales situaciones, conforme al párrafo 6, la Parte requirente deberá ser notificada sin demora, de modo que pueda evaluar si corre el riesgo planteado y sigue adelante con la solicitud de

conservación, o si busca una manera más intrusiva, pero más segura, de procurar la asistencia mutua, como el procedimiento de registro y confiscación.

289. Por último, el párrafo 7 obliga a cada Parte a asegurar que los datos conservados de conformidad con lo dispuesto en este Artículo se conservarán por lo menos 60 días mientras esté pendiente el recibo de la solicitud formal de asistencia mutua en que se pide la revelación de los datos, y seguirán siendo conservados una vez recibida dicha solicitud.

Revelación rápida de datos conservados relativos al tráfico (Artículo 30)

290. Este artículo establece el equivalente internacional de la facultad establecida para el uso a nivel nacional en el Artículo 17. Con frecuencia, a petición de una Parte en la que se cometió un delito, la Parte requerida conservará los datos relativos al tráfico en relación con una transmisión que ha viajado a través de sus ordenadores, con el fin de rastrear la transmisión hasta su origen e identificar al autor del delito, o localizar pruebas esenciales. Al hacerlo, la Parte requerida puede descubrir que los datos relativos al tráfico encontrados en su territorio revelan que la transmisión había sido encaminada desde un proveedor de servicios situado en un tercer Estado, o desde un proveedor de servicios que se encuentra en el mismo Estado requirente. En tales casos, la Parte requerida deberá proporcionar sin demora a la Parte requirente una cantidad suficiente de datos relativos al tráfico que permita la identificación del proveedor de servicios y el trayecto de la comunicación desde el otro Estado. Si la transmisión pasó por un tercer Estado, esta información permitirá a la Parte requirente hacer una solicitud de rápida conservación y asistencia mutua a ese otro Estado a fin de rastrear la transmisión hasta su origen. Si la transmisión ha vuelto al territorio de la Parte requirente, la misma podrá obtener la conservación y la revelación de otros datos relativos al tráfico a través de procesos efectuados a nivel nacional.

291. Conforme al párrafo 2, la Parte requerida podrá negarse a divulgar los datos relativos al tráfico solo cuando su divulgación pudiera atentar contra su soberanía, la seguridad, el orden público u otros intereses fundamentales, o cuando considere que el delito es un delito político o un delito relacionado con un delito político. Al igual que en el Artículo 29 (Conservación rápida de datos informáticos almacenados), en vista de que este tipo de información es tan crucial para identificar a de quienes hayan cometido delitos en el ámbito de este Convenio o localizar pruebas esenciales, los motivos para denegar la revelación deben estar estrictamente limitados, y se acordó que se excluye la posibilidad de considerar cualquier otra base para denegar la asistencia.

Título 2 - Asistencia mutua en relación con los poderes de investigación

Asistencia mutua en relación con el acceso a datos almacenados (Artículo 31)

292. Cada Parte debe tener, para beneficio de la otra Parte, la capacidad de registrar, o acceder de manera similar, y de confiscar, o conseguir de manera similar, y de revelar los datos almacenados por medio de un sistema informático situado en su territorio -- al igual que en virtud del Artículo 19 (Registro y confiscación de datos informáticos almacenados) debe tener la capacidad de hacerlo a nivel nacional. El párrafo 1 autoriza a una Parte a requerir este tipo de asistencia mutua, y el párrafo 2 establece que la Parte requerida debe poder proporcionarla. El párrafo 2 sigue también el principio de que los términos y condiciones para proveer dicha cooperación deberían ser los establecidos en los tratados aplicables, los acuerdos y las leyes nacionales que rigen la asistencia jurídica mutua en materia penal. En virtud del párrafo 3, deberá darse respuesta a dicha solicitud de forma acelerada cuando (1) existen motivos para creer que los datos pertinentes son particularmente vulnerables a sufrir pérdida o modificación, o (2) cuando esos tratados, acuerdos o leyes así lo establezcan.

Acceso transfronterizo a los datos almacenados, con consentimiento o cuando sean accesibles al público (Artículo 32)

293. La cuestión de si una Parte puede acceder de forma unilateral a los datos informáticos almacenados en otra Parte sin solicitar la asistencia mutua fue una cuestión que examinaron detenidamente quienes redactaron el Convenio. Hubo un examen detallado de los casos en los cuales puede ser aceptable que los Estados actúen de manera unilateral y aquellos en los que puede no serlo. En última instancia, quienes redactaron el Convenio determinaron que no era posible todavía elaborar un régimen completo y vinculante desde el punto de vista legal que regule este campo. En parte, esto se debió a la falta de experiencias concretas respecto de este tipo de situaciones hasta la fecha, y, en parte, esto se debió a que se consideró que la solución adecuada a menudo es resultado de las circunstancias concretas de cada caso, lo que hace difícil formular normas generales. En última instancia, los redactores decidieron sólo enunciados en el artículo 32 de la Convención de las situaciones en las que todos coincidimos en que la acción unilateral es admisible. Acordaron no regulan otras situaciones hasta el momento en que la experiencia ha ido obteniendo más y más debates pueden celebrarse a la luz de la misma. En este sentido, el Artículo 39, párrafo 3 establece que no se autorizan ni se excluyen otras situaciones.

294. El Artículo 32 (Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público) aborda dos situaciones: primero, cuando los datos a los que se ha de acceder sean accesibles al

público y segundo, cuando una Parte ha accedido a datos o recibido datos ubicados fuera de su territorio a través de un sistema informático de su territorio y ha obtenido el consentimiento legal y voluntario de la persona que tiene autoridad legal para revelar los datos a la Parte a través de ese sistema. La cuestión de quién está "legítimamente autorizado" a revelar datos puede variar dependiendo de las circunstancias, la naturaleza de la persona y la ley aplicable de que se trate. Por ejemplo, el correo electrónico de una persona puede estar almacenado en otro país por un proveedor de servicios, o una persona puede deliberadamente almacenar datos en otro país. Estas personas pueden recuperar los datos y, siempre que tengan la autoridad legal, pueden voluntariamente revelar los datos a los agentes del orden o permitir a esos funcionarios acceder a los datos, según lo dispuesto en el artículo.

Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico (Artículo 33)

295. En muchos casos, los investigadores no pueden asegurar que sean capaces de rastrear una comunicación hasta su origen, siguiendo la pista a través de los registros de transmisiones anteriores, ya que los datos esenciales relativos al tráfico pueden haber sido eliminados automáticamente por un proveedor de servicios en la cadena de transmisión antes de poder ser conservados. Por lo tanto, es fundamental que los investigadores en cada Parte tengan la capacidad de obtener los datos relativos al tráfico en tiempo real relacionados con las comunicaciones que pasan a través de un sistema informático en otras Partes. Por consiguiente, conforme al Artículo 33 (Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico), cada Parte tiene la obligación de recopilar en tiempo real los datos relativos al tráfico para la otra Parte. Si bien este artículo requiere que las Partes cooperen con estas cuestiones, aquí, como en otros puntos, se da preferencia a las modalidades existentes respecto de la asistencia mutua. Así, los términos y condiciones mediante los cuales se ha de prestar dicha cooperación en general suelen ser los establecidos en los tratados, acuerdos y leyes aplicables que rigen la asistencia jurídica mutua en materia penal.

296. En muchos países, la asistencia mutua se proporciona ampliamente respecto de la obtención en tiempo real de datos relativos al tráfico, porque dicha obtención de datos es considerada menos intrusiva que la interceptación de datos relativos al contenido o el registro y la confiscación. Sin embargo, una serie de Estados han adoptado un enfoque más restringido. En consecuencia, de la misma manera que las Partes pueden formular una reserva conforme al Artículo 14 (Ámbito de aplicación de las disposiciones de procedimiento), párrafo 3, con respecto al alcance de la medida equivalente a nivel nacional, el párrafo 2 permite a las Partes limitar el ámbito de aplicación de esta medida a una serie más restringida de delitos que los establecidos en el Artículo 23 (Principios generales relativos a la cooperación internacional). Se formula una advertencia: en ningún caso la

serie de delitos puede ser más limitada que la serie de delitos para la cual tal medida está disponible en un caso equivalente a nivel nacional. En efecto, debido a que la obtención en tiempo real del los datos relativos al tráfico es a veces la única manera de determinar la identidad del autor de un delito, y debido al carácter menos intrusivo de la medida, el uso de la expresión "al menos" en el párrafo 2 se ha concebido para alentar a las Partes a permitir la asistencia más amplia posible, es decir, incluso en ausencia de doble tipificación penal.

Asistencia mutua en relación con la interceptación de datos relativos al contenido (Artículo 34)

297. Debido al alto grado de intrusividad de la interceptación, la obligación de proveer asistencia mutua para la interceptación de los datos relativos al contenido es restringido. La asistencia se facilitará en la medida que lo permitan las leyes y tratados aplicables de las Partes. Como la prestación de cooperación en los casos de interceptación de contenidos es un área emergente de la práctica de la asistencia mutua, se decidió deferir a los regímenes de ayuda mutua existentes y a las leyes nacionales en lo tocante al alcance y las limitaciones de la obligación de brindar asistencia. En este sentido, se hace referencia a los comentarios sobre los Artículos 14, 15 y 21, así como a la Recomendación núm. R (85) 10 concerniente a la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal respecto de los exhortos para solicitar la interceptación de las telecomunicaciones.

Título 3 - Red 24/7

Red 24/7 (Artículo 35)

298. Como ya se ha discutido previamente, el combatir eficazmente los delitos cometidos mediante el uso de sistemas informáticos y la obtención eficaz de pruebas en formato electrónico exige una respuesta muy rápida. Además, con sólo pulsar unas pocas teclas, puede tener lugar una acción en una parte del mundo que produce instantáneamente muchas consecuencias a muchos miles de kilómetros y atravesando muchas zonas horarias. Por esta razón, la cooperación policial existente y las modalidades de asistencia mutua requieren canales complementarios para abordar eficazmente los desafíos de la era informática. El canal establecido en el presente artículo se basa en la experiencia obtenida con una red que está ya en funcionamiento que fue creada bajo los auspicios de las naciones del grupo G8. Conforme a este artículo, cada Parte tiene la obligación de designar un punto de contacto que esté disponible las 24 horas del día, los 7 días de la semana a fin de asegurar la asistencia inmediata en las investigaciones y los procedimientos en el ámbito de este Capítulo, en particular como lo define el Artículo 35, párrafo 1, acápites a) a c). Se acordó que el establecimiento de esta red es

uno de los más importantes medios previstos por el presente Convenio para asegurar que las Partes puedan responder eficazmente a los desafíos que plantea la aplicación de las leyes respecto de los delitos informáticos o los delitos relacionados con la informática.

299. El punto de contacto 24/7 de cada Parte debe facilitar o directamente llevar a cabo, entre otras cosas, la prestación de asesoramiento técnico, la conservación de datos, la obtención de pruebas, el suministro de información de carácter jurídico, y la localización de sospechosos. El término "información de carácter jurídico" en el párrafo 1 significa asesorar a la otra Parte que solicita la cooperación respecto de cualquier requisito legal necesario para prestar la cooperación, ya sea de manera formal o informal.

300. Cada Parte tiene la libertad de determinar dónde ubicar el punto de contacto dentro de su estructura de aplicación de las leyes. Algunas Partes tal vez deseen ubicar el punto de contacto 24/7 en el seno de su autoridad central encargada de la de asistencia mutua; algunas pueden pensar que la mejor ubicación es en una unidad de policía especializada en la lucha contra los delitos informáticos o los delitos relacionados con la informática; sin embargo, otras opciones pueden ser apropiadas para una Parte en particular, dada su estructura de gobierno y su sistema jurídico. Como el punto de contacto 24/7 debe brindar asesoramiento técnico para detener o rastrear un ataque y también ha de cumplir con las obligaciones de cooperación internacional tales como la localización de sospechosos, no hay una respuesta correcta, y se prevé que la estructura de la red evolucionará con el correr del tiempo. Al designar el punto de contacto nacional, se debe prestar especial consideración a la necesidad de comunicarse con puntos de contactos que utilicen otros idiomas.

301. El párrafo 2 establece que entre las tareas cruciales que ha de llevar a cabo el punto de contacto 24/7 está la capacidad de facilitar la rápida ejecución de aquellas funciones que no puede llevar a cabo en forma directa. Por ejemplo, si el punto de contacto 24/7 de una Parte forma parte de una unidad policial, debe tener la capacidad para coordinar rápidamente con otros componentes pertinentes dentro de su gobierno, tales como la autoridad central encargada de la asistencia mutua o de la extradición a nivel internacional, a fin de que se puedan tomar las medidas apropiadas en cualquier momento del día o de la noche. Además, el párrafo 2 requiere que el punto de contacto 24/7 de cada Parte tenga la capacidad de realizar comunicaciones con otros miembros de la red de forma expeditiva.

302. El párrafo 3 requiere que cada punto de contacto de la red cuente con los equipos adecuados. Para el buen funcionamiento de la red será esencial contar con equipos de teléfono, de fax y de computación modernos, y el sistema deberá contar con otras formas de comunicación y equipos de análisis a medida que avanza la tecnología. El párrafo 3 requiere también que el personal que participa como parte del equipo de una Parte que trabaja en la red reciba una formación adecuada en relación con los delitos

informáticos y los delitos relacionados con la informática y sepa cómo responder eficazmente a los mismos.

Capítulo IV - Cláusulas finales

303. Con algunas excepciones, las disposiciones contenidas en este Capítulo reproducen, en su mayor parte, las "cláusulas finales modelo" de los acuerdos y convenios elaborados en el marco del Consejo de Europa adoptadas por el Comité de Ministros en la 315ª reunión a nivel de Delegados en febrero de 1980. Como la mayoría de los artículos del 36 al 48 utilizan ya el lenguaje habitual de las cláusulas modelo, o están basados en prácticas de larga data en cuanto a la elaboración de tratados en el Consejo de Europa, no requieren comentarios específicos. Sin embargo, ciertas modificaciones de las cláusulas modelo habituales o algunas nuevas disposiciones requieren una explicación. Cabe señalar en este contexto que las cláusulas modelo han sido adoptadas como un conjunto de disposiciones sin carácter vinculante. Como se señala en la introducción a las cláusulas modelo, "estas cláusulas modelo finales tienen la única finalidad de facilitar la tarea de los comités de expertos y evitar las divergencias textuales que no tuvieran ninguna justificación real. El modelo no es en absoluto vinculante y las diferentes cláusulas pueden ser adaptadas para satisfacer casos particulares."

Firma y entrada en vigor (Artículo 36)

304. El Artículo 36, párrafo 1, se ha redactado siguiendo diversos precedentes establecidos en otros convenios elaborados en el seno del Consejo de Europa, por ejemplo, el Convenio sobre traslado de personas condenadas (STE núm. 112) y el Convenio relativo al blanqueo, embargo y decomiso de los productos del delito (STE núm. 141), que permiten ser firmados, antes de su entrada en vigor, no sólo por los Estados miembros del Consejo de Europa, sino también por los Estados no miembros que hayan participado en su elaboración. La disposición está destinada a permitir que el máximo número de Estados interesados, no sólo los que sean miembros del Consejo de Europa, se constituyan en Partes lo más rápido posible. En este caso, la disposición pretende abarcar cuatro Estados no miembros, Canadá, Japón, Sudáfrica y los Estados Unidos de América, que participaron activamente en la elaboración de la Convención. Una vez que el Convenio entre en vigor, de conformidad con el párrafo 3, otros Estados no miembros no cubiertos por esta disposición podrán ser invitados a adherirse al Convenio, de conformidad con el Artículo 37, párrafo 1.

305. El artículo 36, párrafo 3, establece en 5 el número de ratificaciones, aceptaciones o aprobaciones requeridas para la entrada en vigor del Convenio. Esa cifra es superior al límite usual (3) en los tratados del Consejo de Europa, y refleja la convicción de que es necesario un grupo un poco más numeroso de Estados para empezar a abordar con éxito el desafío que

plantean los delitos informáticos y los delitos relacionados con la informática. Sin embargo, el número no es demasiado elevado como para no retrasar innecesariamente la entrada en vigor de este Convenio. Entre los cinco estados iniciales, al menos tres deben ser miembros del Consejo de Europa, pero los otros dos podrían provenir de los cuatro Estados no miembros que participaron en la elaboración del Convenio. Esta disposición, por supuesto, también permite que el Convenio entre en vigor sobre la base de las expresiones de consentimiento respecto de su obligatoriedad por parte de cinco Estados miembros del Consejo de Europa.

Adhesión al Convenio (artículo 37)

306. El artículo 37 también ha sido redactado en base a los precedentes establecidos en otros convenios del Consejo de Europa, pero con un elemento adicional expreso. En virtud de una práctica de larga data, el Comité de Ministros decide, por propia iniciativa o por pedido, invitar a un Estado no miembro, que no haya participado en la elaboración del Convenio, a adherirse al mismo después de haber consultado a todas las Partes contratantes, sean o no Estados miembros. Esto implica que si algunas de las Partes objeta la adhesión del Estado no miembro, el Comité de Ministros en general no lo invitaría a unirse al convenio. Sin embargo, en virtud de la formula habitual, el Comité de Ministros podría, en teoría, invitar a dicho Estado no miembro a adherirse a un convenio, incluso si un Estado no miembro que es Parte objetara su adhesión. Esto significa que, en teoría, en general no se concede ningún derecho a veto a los Estados no miembros que son Parte en el proceso de extensión de los tratados del Consejo de Europa a otros Estados no miembros. Sin embargo, se ha insertado el requisito expreso de que el Comité de Ministros consulte y obtenga el consentimiento unánime de todos los Estados contratantes - no sólo el de los Estados miembros del Consejo de Europa - antes de invitar a un Estado no miembro a acceder al Convenio. Como se indicó anteriormente, este requisito es coherente con la práctica y reconoce que todos los Estados contratantes de la Convención debe ser capaces de determinar con cuáles Estados no miembros van a entrar en relaciones en virtud de un tratado. Sin embargo, la decisión formal de invitar a un Estado no miembro a adherirse se tomará, conforme con la práctica usual, por parte de los representantes de las Partes Contratantes facultadas para formar parte del Comité de Ministros. Esta decisión requiere de dos tercios de la mayoría prevista en el artículo 20.d de los Estatutos del Consejo de Europa y el voto unánime de los representantes de las Partes Contratantes facultadas para formar parte del Comité.

307. Los Estados federales que deseen adherirse al Convenio, que tengan la intención de hacer una declaración en virtud del Artículo 41, están obligados a presentar por adelantado un borrador de la declaración contemplada en el Artículo 41, párrafo 3, de modo que las Partes puedan evaluar la manera en que la aplicación de la cláusula federal podría afectar la aplicación del Convenio por una futura Parte (véase el párrafo 320).

Efectos del Convenio (Artículo 39)

308. El Artículo 39, párrafos 1 y 2 aborda la relación del Convenio con otros acuerdos o convenios internacionales. El tema de cómo los convenios del Consejo de Europa deberían relacionarse entre sí o con otros tratados, bilaterales o multilaterales, celebrados fuera del ámbito del Consejo de Europa no es abordado por las cláusulas modelo mencionadas *supra.* El enfoque habitual utilizado en los convenios del Consejo de Europa en el ámbito del derecho penal (por ejemplo, el Acuerdo sobre tráfico ilícito por mar (STE núm. 156)) es disponer que: 1) los nuevos convenios no afectan los derechos y obligaciones derivados de los actuales las convenios multilaterales internacionales existentes concernientes a cuestiones especiales; 2) Las partes contratantes de un nuevo convenio podrán celebrar acuerdos bilaterales o multilaterales entre sí respecto de las cuestiones tratadas por el convenio a los fines de complementar o consolidar sus disposiciones o facilitar la aplicación de los principios contenidos en las mismas, y 3) Si dos o más Partes contratantes del nuevo convenio han celebrado ya un acuerdo o tratado respecto de un tema que es abordado en el convenio o han establecido de otro modo sus relaciones respecto de ese tema, estarán facultadas a aplicar dicho acuerdo o tratado o a regular dichas relaciones en consecuencia, en lugar del nuevo convenio, siempre que ello facilite la cooperación internacional.

309. En vista de que el Convenio en general tiene la finalidad de complementar y no de reemplazar a los acuerdos bilaterales y multilaterales celebrados entre las Partes, quienes redactaron el Convenio consideraron que no era particularmente instructiva la posibilidad de limitar la referencia a "cuestiones especiales" y les preocupaba que pudiera causar confusiones innecesarias. En cambio, el párrafo 1 del Artículo 39 indica simplemente que el presente Convenio complementa a otros tratados o acuerdos aplicables celebrados entre las Partes y menciona en concreto tres tratados del Consejo de Europa como ejemplos no exhaustivos: el Convenio Europeo de Extradición de 1957 (STE núm. 24) , el Convenio Europeo en Materia Penal de 1959 (STE núm. 30) y su Protocolo Adicional de 1978 (STE núm. 99). Por consiguiente, respecto de las cuestiones de carácter general, tales acuerdos deberían en principio ser aplicados por las Partes en el Convenio sobre la ciberdelincuencia. En cuanto a cuestiones específicas sólo consideradas en el presente Convenio, la regla de interpretación de *lex specialis derogat legi generali* establece que las Partes deben dar prioridad a las normas contenidas en el Convenio. Un ejemplo es el Artículo 30, que establece la rápida revelación de los datos relativos al tráfico conservados cuando sean necesarios para identificar el trayecto de una comunicación específica. En este ámbito específico, el Convenio, como *lex specialis*, debería establecer una norma de primer recurso sobre las disposiciones en los acuerdos de asistencia mutua más generales.

310. Del mismo modo, quienes redactaron el Convenio consideraron que la adopción de un lenguaje por el cual la aplicación de los acuerdos existentes o futuros serían contingentes de si "fortalecen" o "facilitan" la cooperación podría ser problemática porque, en virtud del enfoque establecido en el Capítulo sobre cooperación internacional, la presunción es que Partes aplicarán los acuerdos y arreglos internacionales pertinentes.

311. Cuando exista un tratado de asistencia mutua o un acuerdo como base para la cooperación, el presente Convenio sólo complementaría, en caso necesario, las normas existentes. Por ejemplo, este Convenio establecería la transmisión de solicitudes de asistencia mutua por medios de comunicación rápidos (véase el Artículo 25, párrafo 3) si esa posibilidad no existe en virtud del tratado o acuerdo original.

312. En consonancia con la naturaleza complementaria del Convenio y, en particular, su enfoque respecto de la cooperación internacional, el párrafo 2 establece que las Partes son también libres de aplicar los acuerdos que ya están en vigor o los que en un futuro puedan entrar en vigor. El precedente para dicha articulación se encuentra en el Convenio sobre el traslado de personas condenadas (STE núm. 112). Ciertamente, en el contexto de la cooperación internacional, se espera que la aplicación de otros acuerdos internacionales (muchos de los cuales ofrecen fórmulas probadas y de larga data para la asistencia internacional) promoverán de hecho la cooperación. De conformidad con los términos del presente Convenio, las Partes pueden también acordar aplicar sus disposiciones sobre cooperación internacional en lugar de esos otros acuerdos (véase el acápite 1) del Artículo 27). En tales circunstancias, las principales disposiciones sobre cooperación establecidas en el Artículo 27 vendrían a reemplazar las normas pertinentes en esos otros acuerdos. En vista de que el presente Convenio en general establece obligaciones mínimas, el Artículo 39, párrafo 2 reconoce que las Partes son libres de asumir las obligaciones que sean más específicas, además de aquellas ya establecidas en el Convenio, al establecer sus relaciones concernientes a los asuntos tratados en el mismo. Sin embargo, esto no es un derecho absoluto: las Partes deben respetar los objetivos y principios del Convenio al hacerlo y, por consiguiente, no pueden aceptar obligaciones que pudieran frustrar su finalidad.

313. Además, al determinar la relación del Convenio con otros acuerdos internacionales, quienes lo redactaron convinieron que las Partes pueden buscar lineamientos adicionales respecto de las disposiciones pertinentes de la Convención de Viena sobre el Derecho de los Tratados.

314. Si bien el Convenio establece un nivel de armonización muy necesario, no pretende abordar todas las cuestiones pendientes relacionadas con los delitos informáticos y con los delitos relacionados con la informática. Por consiguiente, se insertó el párrafo 3 para dejar en claro que el Convenio afecta sólo a los temas que aborda. No están afectados otros derechos, restricciones, obligaciones y responsabilidades que puedan existir, pero que

no son tratados por el Convenio. Se pueden encontrar precedentes de este tipo de cláusulas "de salvedad" en otros acuerdos internacionales (por ej., la Convención de las Naciones Unidas sobre la financiación del terrorismo).

Declaraciones (Artículo 40)

315. El Artículo 40 se refiere a ciertos artículos, mayormente respecto de los delitos establecidos por el Convenio en la sección sobre derecho sustantivo, donde se permite a las Partes incluir algunos elementos específicos adicionales que modifican el ámbito de aplicación de las disposiciones. Dichos elementos adicionales tienen la finalidad de resolver ciertas diferencias conceptuales o jurídicas, que en un tratado de alcance mundial están más justificadas de lo que en realidad debieran ser dentro del contexto exclusivo del Consejo de Europa. Las declaraciones son consideradas aceptables interpretaciones de las disposiciones del Convenio y deberían distinguirse de las reservas, que permiten que una Parte excluya o modifique el efecto legal de ciertas obligaciones establecidas en el Convenio. Puesto que es importante para las Partes en el Convenio saber cuáles elementos adicionales, de haber alguno, han sido adjuntados por otras Partes, existe la obligación de declararlos ante el Secretario General del Consejo de Europa al momento de la firma o al depositar el instrumento de ratificación, aceptación, aprobación o adhesión. Dicha notificación es particularmente importante con respecto a la definición de los delitos, ya que la condición de doble tipificación penal tendrán que ser satisfecha por las Partes al aplicar ciertas facultades procesales. No se estableció ningún límite numérico respecto de las declaraciones.

Cláusula federal (Artículo 41)

316. En consonancia con el objetivo de permitir que el mayor número posible de Estados lleguen a ser Partes del Convenio, el Artículo 41 permite formular una reserva que tiene como finalidad allanar las dificultades que los Estados federales pueden enfrentar como resultado de la distribución de poderes entre autoridades centrales y regionales que los caracteriza. Existen precedentes fuera del ámbito del derecho penal respecto de declaraciones o reservas federales a otros acuerdos internacionales[11]. Aquí, el Artículo 41 reconoce que pueden ocurrir variaciones de menor importancia en cuanto al alcance como resultado de las leyes nacionales y de las prácticas bien establecidas de una Parte que es un Estado federal. Dichas variaciones deben estar basadas en su Constitución o en otros principios fundamentales

[11] P. ej, la Convención sobre el Estatuto de los Refugiados, del 28 de julio de 1951, art. 34; la Convención sobre el Estatuto de los Apátridas, del 28 de septiembre de 1954, art. 37; Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras, del 10 de junio de 1958, art. 11; el Convenio para la Protección del Patrimonio Mundial Cultural y Natural, del 16 de noviembre de 1972, art. 34.

relativos a la división de poderes en materia de justicia penal entre el gobierno central y los estados constituyentes o las entidades territoriales de un Estado federal. Hubo acuerdo entre quienes redactaron el Convenio respecto de que la aplicación de la cláusula federal sólo conduciría a variaciones menores en la aplicación del Convenio.

317. Por ejemplo, en los Estados Unidos, en virtud de su Constitución y los principios fundamentales del federalismo, la legislación penal federal en general regula la conductas basándose en sus efectos sobre el comercio interestatal o extranjero, mientras que los asuntos de poca trascendencia o puramente locales están tradicionalmente reguladas por los estados constituyentes. Este enfoque del federalismo aún proporciona una cobertura amplia de las conductas ilícitas comprendidas en este Convenio en virtud del derecho penal federal de los EE.UU., pero reconoce que los estados constituyentes continuarán regulando las conductas que sólo tienen un impacto menor o sean de carácter puramente local. En algunos casos, dentro de esa categoría limitada de conductas reguladas por las leyes de los estados y no por las leyes federales, un estado constituyente puede no prever una medida que de otro modo estaría comprendida en el ámbito de aplicación del presente Convenio. Por ejemplo, un ataque a un ordenador personal independiente, o a una red de ordenadores conectados entre sí en un solo edificio, puede ser considerado delito penal sólo si así lo contemplan las leyes del estado en el que tuvo lugar el ataque; sin embargo, el ataque constituiría un delito federal si el acceso al ordenador tuvo lugar a través de Internet, ya que el uso de Internet tiene un efecto sobre el comercio interestatal o extranjero, elemento necesario para invocar las leyes federales. La aplicación de este Convenio a través de las leyes federales de los Estados Unidos, o por medio de las leyes de otro estado federal, en circunstancias similares, estaría en conformidad con los requisitos del Artículo 41.

318. El ámbito de aplicación de la cláusula federal se ha limitado a las disposiciones del Capítulo II (Derecho penal sustantivo, derecho procesal y jurisdicción). Los Estados federales que se acojan a esta disposición todavía seguirían teniendo la obligación de cooperar con las otras Partes en virtud del Capítulo III, aun cuando el estado constituyente u otra entidad territorial similar en el que se encuentren un fugitivo o las pruebas no tipifique como delito esta conducta ni requiera trámites legales en virtud de este Convenio.

319. Además, el párrafo 2 del Artículo 41 dispone que un Estado federal, al formular una reserva en virtud del párrafo 1 del presente Artículo, no puede aplicar los términos de dicha reserva para excluir o disminuir sustancialmente sus obligaciones de establecer las medidas establecidas en el Capítulo II. En general, se deberá proporcionar una capacidad amplia y eficaz para hacer cumplir la ley con respecto a esas medidas. En cuanto a las disposiciones cuya aplicación sea de la competencia legislativa de los estados constituyentes o de otras entidades territoriales similares, el gobierno federal remitirá las disposiciones a las autoridades de esas entidades con su visto

bueno, y las alentará a tomar las medidas apropiadas para lograr su aplicación.

Reservas (Artículo 42)

320. El artículo 42 establece una serie de reservas posibles. Este enfoque deriva del hecho de que el Convenio abarca un área del derecho penal y del derecho procesal penal, que es relativamente nueva para muchos Estados. Además, la naturaleza global del Convenio, que estará abierto para la firma de los Estados miembros y no miembros del Consejo de Europa, hace necesario contar con la posibilidad de hacer dichas reservas. Estas posibilidades de reserva tienen la finalidad de permitir que el mayor número posible de Estados lleguen a ser Partes del Convenio, al mismo tiempo que permiten a dichos Estados mantener ciertos enfoques y conceptos que sean coherentes con su legislación nacional. Al mismo tiempo, quienes redactaron el Convenio procuraron restringir las posibilidades de hacer reservas con el fin de asegurar en la mayor medida posible la aplicación uniforme del Convenio por las Partes. Por lo tanto, no se puede hacer ninguna otra reservas con excepción de las enumeradas. Además, las reservas pueden efectuarse sólo por una Parte al momento de firmar o al depositar sus instrumentos de ratificación, aceptación, aprobación o adhesión.

Mantenimiento y retirada de las reservas (Artículo 43)

321. Reconociendo que para algunas Partes ciertas reservas son esenciales para evitar conflictos con sus principios jurídicos fundamentales o constitucionales, el Artículo 43 no impone ningún límite de tiempo específico para la retirada de las reservas. En cambio, deberían retirarse tan pronto como las circunstancias lo permitan.

322. A fin de mantener cierta presión sobre las Partes y de hacerlas al menos considerar la posibilidad de retirar sus reservas, el Convenio autoriza al Secretario General del Consejo de Europa a indagar periódicamente respecto de la posibilidad de que se retire alguna reserva. Esta posibilidad de consulta es una práctica corriente en virtud de varios de diversos instrumentos del Consejo de Europa. Las Partes tienen así una oportunidad para indicar si todavía necesitan mantener sus reservas con respecto a ciertas disposiciones y a retirar, posteriormente, las que ya no sean necesarias. Se espera que con el correr del tiempo las Partes puedan eliminar tantas reservas como les sea posible a fin de promover la aplicación uniforme del Convenio.

Enmiendas (Artículo 44)

323. El artículo 44 tiene su precedente en el Convenio relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito (STE núm.

141), donde se introdujo como una innovación respecto de los convenios de derecho penal elaborados en el marco del Consejo de Europa. El procedimiento de enmienda está concebido principalmente para cambios relativamente menores de carácter procesal y técnico. Quienes redactaron el Convenio consideraron que podrían efectuarse cambios importantes en el Convenio adoptando protocolos adicionales.

324. Las propias Partes pueden examinar la necesidad de incluir enmiendas o protocolos conforme al procedimiento de consulta establecido en el Artículo 46. El Comité europeo para los problemas criminales (CDPC) deberá ser informado periódicamente al respecto y tendrá la obligación de adoptar las medidas necesarias para asistir a las Partes en sus esfuerzos por modificar o complementar el Convenio.

325. De conformidad con el párrafo 5, toda enmienda aprobada entraría en vigor sólo cuando todas las Partes hayan informado de su aceptación al Secretario General. Este requisito tiene por objeto garantizar que el Convenio evolucionará de manera uniforme.

Solución de controversias (Artículo 45)

326. El Artículo 45, párrafo 1, establece que el Comité Europeo para Asuntos Delictivos (CDPC) debería mantenerse informado respecto de la interpretación y la aplicación de las disposiciones del Convenio. El párrafo 2 impone a las Partes la obligación de buscar una solución pacífica de cualquier controversia concerniente a la interpretación o la aplicación del Convenio. Todo procedimiento de solución de controversias debería ser acordados entre las Partes interesadas. Se sugirieron tres posibles mecanismos para la solución de controversias: el propio Comité europeo para los problemas criminales (CDPC), un tribunal arbitral o la Corte Internacional de Justicia.

Consultas entre las Partes (Artículo 46)

327. El artículo 46 crea un marco para que las Partes puedan efectuar consultas respecto de la aplicación del Convenio, el efecto de importantes desarrollos tecnológicos, legales y de política relacionados con el tema de los delitos informáticos o los delitos relacionados con la informática y la obtención de pruebas en formato electrónico, y la posibilidad de complementar o enmendar el Convenio. Las consultas examinarán en particular cuestiones que han surgido en cuanto al uso y la aplicación del Convenio, incluidos los efectos de las declaraciones y reservas formuladas en virtud de los Artículos 40 y 42.

328. El procedimiento es flexible y se deja a criterio de las Partes decidir cómo y cuándo reunirse, si así lo desean. Quienes redactaron el Convenio consideraron necesario este procedimiento para garantizar que pudieran

estar involucradas todas las Partes en el Convenio, incluso los Estados no miembros del Consejo de Europa, en igualdad de condiciones, respecto de cualquier mecanismo de seguimiento y preservar al mismo tiempo las competencias del Comité europeo para los problemas criminales (CDPC). Este último no sólo deberá mantenerse informado regularmente respecto de las consultas que tienen lugar entre las Partes, sino que también las facilitará y tomará todas las medidas necesarias para asistir a las Partes en sus respectivos esfuerzos para completar o modificar el Convenio. Teniendo en cuenta las necesidades de una prevención eficaz y de iniciar acciones judiciales eficaces respecto de los delitos informáticos y las cuestiones de privacidad conexas, el impacto potencial sobre las actividades comerciales y otros factores pertinentes, pueden ser útiles las opiniones de las partes interesadas, incluidas las organizaciones encargadas de la aplicación de las leyes, las organizaciones no gubernamentales y las del sector privado (véase también el párrafo 14).

329. El párrafo 3 establece un examen del funcionamiento del Convenio después de 3 años de su entrada en vigor, pudiendo recomendarse en ese momento las enmiendas que se estimen oportunas. El CDPC llevará a cabo ese examen con la asistencia de las Partes.

330. El párrafo 4 señala que, salvo cuando se haga cargo el Consejo de Europa, las propias Partes deberán financiar todas las consultas que se efectúen de conformidad con el párrafo 1 del Artículo 46. Sin embargo, además del Comité europeo para los problemas criminales (CDPC), el Secretario del Consejo de Europa prestará asistencia a las Partes en los esfuerzos que realicen en virtud del Convenio.