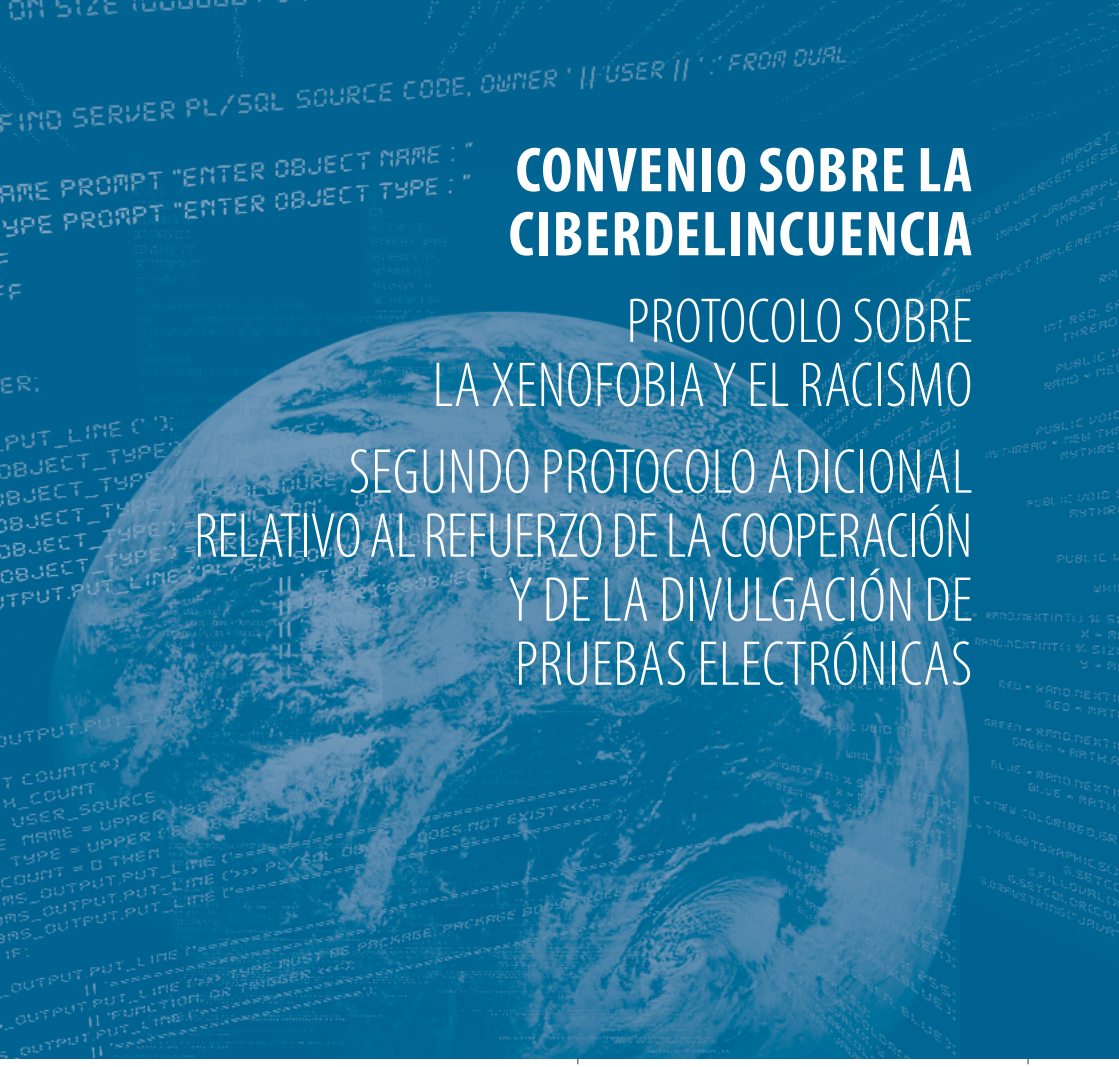

CONVENIO SOBRE LA CIBERDELINCUENCIA

PROTOCOLO SOBRE LA XENOFOBIA Y EL RACISMO

SEGUNDO PROTOCOLO ADICIONAL RELATIVO AL REFUERZO DE LA COOPERACIÓN Y DE LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS

Informe explicativo
y Notas de orientacion

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CONVENIO SOBRE LA CIBERDELINCUENCIA

PROTOCOLO SOBRE LA XENOFOBIA Y EL RACISMO

SEGUNDO PROTOCOLO ADICIONAL RELATIVO AL REFUERZO DE LA COOPERACIÓN Y DE LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS

Informe explicativo
Notas de orientación

Consejo de Europa

Portada y maquetación:
Departamento de producción de documentos y publicaciones (DPDP), Consejo de Europa

Impresión: Consejo de Europa

Índice

Convenio sobre la ciberdelincuencia (STE núm. 185)

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio;

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad contra la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos, y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;

Convencidos de que el presente Convenio es necesario para prevenir los actos encaminados a socavar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección,

investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (l950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (l966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin injerencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, en el Convenio del Consejo de Europa de l98l para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (l989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (l999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de hacer más eficaces las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las recomendaciones del Comité de Ministros núm. R (85) l0 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal, en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones; núm. R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines; núm. R (87) l5 relativa a la regulación de la utilización de datos personales por la policía; núm. R (95) 4 sobre la protección de los datos personales en el ámbito

de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, así como núm. R (89) 9 sobre la delincuencia relacionada con la informática, que proporciona directrices a los legisladores nacionales para la definición de determinados delitos informáticos, y núm. R (95) l3 sobre los problemas de derecho procesal en relación con la tecnología de la información.

Teniendo en cuenta la Resolución núm. l, adoptada por los Ministros de Justicia europeos en su XXI Conferencia (Praga, 10 y 11 de junio de l997), que recomienda al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo para los Problemas Criminales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución núm. 3, adoptada en la XXIII Conferencia de Ministros de Justicia europeos (Londres, 8 y 9 de junio de 2000), que alienta a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconoce la necesidad de un sistema rápido y eficaz de cooperación internacional que refleje debidamente las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con motivo de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de l997), con el fin de hallar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

Capítulo I - Terminología

Artículo 1 -Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa., y

b. por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c. por "proveedor de servicios" se entenderá:

i. toda entidad pública o privada que brinde a los usuarios de sus servicios la posibilidad de comunicarse entre sí por medio de un sistema informático, y

ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio, y

d. por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Capítulo II - Medidas que deberán adoptarse a nivel nacional

Sección 1 -Derecho penal sustantivo

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

Artículo 2 - Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3 - Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no publicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 - Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el párrafo 1 provoquen daños graves.

Artículo 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 - Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

   i. un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5, y

   ii. una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático,

con el fin de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5, y

b. la posesión de alguno de los elementos contemplados en los anteriores incisos i) o ii) del apartado a) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización,

importación, difusión u otra forma de puesta a disposición mencionadas en el párrafo 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el párrafo 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el inciso ii) del apartado a) del párrafo 1del presente artículo.

Título 2 -Delitos informáticos

Artículo 7 - Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 - Fraude informático

Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a. cualquier introducción, alteración, borrado o supresión de datos informáticos, y

b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para terceros.

Título 3 – Delitos relacionados con el contenido

Artículo 9 - Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos

a. la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b. la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c. la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para terceros, y

e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del anterior párrafo 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:

a. un menor comportándose de una forma sexualmente explícita;

b. una persona que parezca un menor comportándose de una forma sexualmente explícita, e

c. imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3. A los efectos del anterior párrafo 2, por "menor" se entenderá toda persona menor de l8 años de edad. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en su totalidad o en parte, los apartados d) y e) del párrafo 1, y los apartados b) y c) del párrafo 2.

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

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

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de l97l por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, y

del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativa y de otro tipo que sean necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y de sanciones

Artículo 11 - Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a l0 del presente Convenio, con la intención de que se cometa ese delito.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de los delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.l.a) y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en su totalidad o en parte, el párrafo 2 del presente artículo.

Artículo 12 - Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:

a. un poder de representación de la persona jurídica;

b. una autorización para tomar decisiones en nombre de la persona jurídica, y

c. una autorización para ejercer funciones de control en la persona jurídica.

2. Además de los casos ya previstos en el párrafo 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el párrafo 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.

3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídico podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13 - Sanciones y medidas

Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2 -Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 - Ámbito de aplicación de las disposiciones sobre procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con miras a establecer los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo que se establezca lo contrario en el artículo 2l, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;

b. a cualquier otro delito cometido por medio de un sistema informático, y

c. a la obtención de pruebas electrónicas de cualquier delito.

3.a. Cada Parte podrá reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 2l. Las Partes tratarán de limitar tal reserva de modo que sea posible la la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 2l a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

   i. que se haya puesto en funcionamiento para grupo restringido de usuarios, y

   ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 2l.

Artículo 15 - Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente sección se sometan las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y de las libertades fundamentales (l950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (l966), u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Título 2 – Conservación rápida de datos informáticos almacenados

Artículo 16- Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos son especialmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el anterior párrafo 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en poder o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para obligar a esa persona a conservar y proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días,

de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos l4 y l5.

Artículo 17 - Conservación y revelación parcial rápidas de datos sobre el trafico

1. Con el fin de garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 6, cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias:

a. para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y

b. para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos l4 y l5.

Título 3 – Orden de presentación

Artículo 18 - Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con objeto de facultar a sus autoridades competentes para que ordenen:

a. a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento de datos informáticos, y

b. a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos l4 y l5.

3. A los efectos del presente artículo, por "datos relativos a los abonados" se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

a. el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios, y

c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Título 4 – Registro y confiscación de datos informáticos almacenados

Artículo 19 - Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con objeto de facultar a sus autoridades competentes para que registren o tengan acceso de una forma similar:

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo, y

b. a un dispositivo de almacenamiento de datos informáticos que permita almacenar datos informáticos, en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático especifico o a una parte del mismo, de conformidad con lo dispuesto en el apartado a) del párrafo 1, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con objeto de facultar a sus autoridades competentes para que confisquen u obtengan de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los párrafos 1 ó 2. Estas medidas incluirán las siguientes facultades:

a. confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento de datos informáticos;

b. realizar y conservar una copia de dichos datos informáticos;

c. preservar la integridad de los datos informáticos almacenados de que se trate, y

d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con objeto de facultar a sus autoridades competentes para que ordenen a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos l4 y l5.

Título 5 – Obtención en tiempo de datos informáticos

Artículo 20 - Obtención en tiempo real de datos sobre el trafico

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con objeto de facultar a sus autoridades competentes para que:

a. obtengan o graben mediante la aplicación de medios técnicos existentes en su territorio, y

b. obliguen a un proveedor de servicios, dentro de los límites de su capacidad técnica, a:

   i. obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

   ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el tráfico asociados a comunicaciones especificas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado a) del párrafo 1, podrá adoptar en su lugar las medidas legislativas y de otro tipo que sean necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará 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.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos l4 y l5.

Artículo 21 - Interceptación de datos sobre el contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con objeto de facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno, para que:

a. obtengan o graben mediante la aplicación de medios técnicos existentes en su territorio, y

b. obliguen un proveedor de servicios, dentro de los límites de su capacidad técnica, a:

   i. obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o

   ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado a) del párrafo 1, podrá adoptar en su lugar las medidas legislativas y de otro tipo que sean necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará 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.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos l4 y l5.

Sección 3 -Jurisdicción

Artículo 22 - Jurisdicción

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a. en su territorio, o

b. a bordo de un buque que enarbole el pabellón de dicha Parte, o

c. a bordo de una aeronave matriculada según las leyes de dicha Parte, o

d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Cualquier Estado podrá reservarse el derecho a no aplicar, o a aplicar únicamente en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados b) y d) del párrafo 1 del presente artículo o en cualquier otra parte de los mismos.

3. Cada Parte adoptará las medidas que sean necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el párrafo 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar la jurisdicción más adecuada para las actuaciones penales.

Capítulo III - Cooperación internacional

Sección 1 - Principios generales

Título 1 -Principios

Artículo 23 - Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca, y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Título 2 – Principios relativos a la extradición

Artículo 24 - Extradición

1.a. El presente artículo se aplicara a la extradición entre las Partes por los delitos establecidos en los artículos 2 a ll del presente Convenio, siempre que estén penalizados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de al menos un año, o con una pena más severa.

b. Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE núm. 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.

2. Se considerará que los delitos mencionados en el párrafo 1 del presente artículo figuran entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el párrafo 1 del presente artículo.

4 Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Cuando se deniegue la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a solicitud de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informara a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y llevarán a cabo sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7.a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3 – Principios generales relativos a la asistencia mutua

Artículo 25 - Principios generales relativos a la asistencia mutua

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos, o para la obtención de pruebas en formato electrónico de un delito.

2. Cada Parte adoptará también las medidas legislativas y de otro tipo que sean necesarias para cumplir las obligaciones establecidas en los artículos 27 a 35.

3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, según sea necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y responderá a la misma por cualquiera de estos medios rápidos de comunicación.

4. Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos, o lo denomine o no con la misma terminología que la Parte requirente.

Artículo 26 - Información espontánea

1. Dentro de los límites de su derecho interno, y sin solicitud previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio, o podría dar lugar a una solicitud de cooperación de dicha Parte en virtud del presente capítulo.

2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que entonces deberá determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

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

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

1. Cuando entre las Partes requirente y requerida no se esté vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los párrafos 2 a 9 del presente artículo. Las disposiciones del presente artículo no serán aplicables cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2.a. Cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.

b. Las autoridades centrales se comunicarán directamente entre sí.

c. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y las direcciones de las autoridades designadas en cumplimiento del presente párrafo .

d. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.

4. Además de las condiciones o de los motivos de denegación contemplados en el párrafo 4 del artículo 25, la Parte requerida podrá denegar la asistencia si:

a. la solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político, y

b. considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden publico u otros intereses esenciales.

5. La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

7. La Parte requerida informará sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

8. La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede dar curso a esa solicitud de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.

9.a. En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b Cualquier solicitud o comunicación en virtud de este párrafo podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

c. Cuando se presente una solicitud en aplicación del apartado a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informara directamente a la Parte requirente de dicha remisión.

d. Las solicitudes y comunicaciones efectuadas en virtud del presente párrafo que no impliquen medidas coercitivas podrán remitirse directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e. En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario

General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.

Artículo 28 - Confidencialidad y restricción de la utilización

1. En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán aplicables cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:

a. se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o

b. no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.

3. Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el párrafo 2, informará de ello sin demora a la otra Parte, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedará vinculada por ella.

4. Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el párrafo 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material.

Sección 2 - Disposiciones especiales

Título 1 – Asistencia mutua en materia de medidas provisionales

Artículo 29 - Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de

asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

2. En las solicitudes de conservación que se formulen en virtud del párrafo 1 se indicará:

a. la autoridad que solicita dicha conservación;

b. el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c. los datos informáticos almacenados que deben conservarse y su relación con el delito;

d. cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;

e. la necesidad de la conservación, y

f. que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a ll del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si:

a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político o

b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden publico u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por si sola no bastará para garantizar la futura disponibilidad de los datos, o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.

7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el párrafo 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, de confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

Artículo 30 - Revelación rápida de datos conservados sobre el trafico

1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

2. La revelación de datos sobre el tráfico en virtud del párrafo 1 únicamente podrá denegarse si:

a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político, o

b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden publico u otros intereses esenciales.

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

Artículo 31 - Asistencia mutua en relación con el acceso a datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.

2. La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.

3. Se dará curso a la solicitud lo antes posible cuando:

a. existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación, o

b. los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean la cooperación rápida.

Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al publico

Una Parte podrá, sin autorización de otra Parte:

a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos, o

b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones especificas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el párrafo 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34 - Asistencia mutua relativa a la interceptación de datos sobre el contenido

Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas

transmitidas por medio de un sistema informático, en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Título 3 – Red 24/7

Artículo 35 - Red 24/7

1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a. el asesoramiento técnico;

b. la conservación de datos en aplicación de los artículos 29 y 30, y

c. la obtención de pruebas, el suministro de información de carácter jurídico y la localización de sospechosos.

2.a. El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

b. Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV - Disposiciones finales

Artículo 36 - Firma y entrada en vigor

1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán ante el Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los párrafos 1 y 2.

4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los párrafos 1 y 2.

Artículo 37 - Adhesión al Convenio

1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior párrafo l, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión ante el Secretario General del Consejo de Europa.

Artículo 38 - Aplicación territorial

1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.

2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos párrafos anteriores podrá retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación.

Artículo 39 - Efectos del Convenio

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

- el Convenio Europeo de Extradición, abierto a la firma en París el l3 de diciembre de l957 (STE núm. 24);
- el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de l959 (STE núm. 30);
- el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el l7 de marzo de l978 (STE núm. 99).

2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de las Partes.

Artículo 40 - Declaraciones

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículos 2, 3, 6.l.b), 7, 9.3 y 27.9.e).

Artículo 41 - Clausula federal

1. Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los Estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.

2. Cuando formule una reserva en aplicación del párrafo 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.

3. Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informará de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42 - Reservas

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, párrafo 3 del artículo 6, párrafo 4 del artículo 9, párrafo 3 del artículo l0, párrafo 3 del artículo 11, párrafo 3 del artículo 14, párrafo 2 del artículo 22, párrafo 4 del artículo 29 y párrafo 1 del artículo 4l. No podrán formularse otras reservas.

Artículo 43 - Situación de las reservas y retirada de las mismas

1. La Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla en su totalidad o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica que la retirada de una reserva surtirá efecto en una fecha especificada en la misma y ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior.

2. La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirará dicha reserva, en su totalidad o en parte, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44 - Enmiendas

1. Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo para los Problemas Criminales (CDPC), que presentará al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el párrafo 3 del presente artículo será remitido a las Partes para su aceptación.

5. Cualquier enmienda adoptada de conformidad con el párrafo 3 del presente artículo entrará en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45 - Solución de controversias

1. Se mantendrá informado al Comité Europeo para los Problemas Criminales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacifico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones

serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46 - Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar:

a. la utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;

b. el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico, y

c. el estudio de la conveniencia de ampliar o enmendar el presente Convenio.

2. Se mantendrá periódicamente informado al Comité Europeo para los Problemas Criminales (CDPC) acerca del resultado de las consultas mencionadas en el párrafo 1.

3. Cuando proceda, el CDPC facilitará las consultas mencionadas en el párrafo 1 y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo para los Problemas Criminales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes.

4. Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el párrafo 1 serán sufragados por las Partes en la forma que éstas determinen.

5. Las Partes contarán con la asistencia de la Secretaria del Consejo de Europa a la hora de desempeñar sus funciones en aplicación del presente artículo.

Artículo 47 - Denuncia

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48 - Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

a. cualquier firma;

b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;

d. cualquier declaración formulada en virtud del artículo 40 o reserva formulada de conformidad con el artículo 42, y

e. cualquier otro acto, notificación o comunicación relativo al presente Convenio. En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa El Secretario General del Consejo de Europa remitirá copias certificadas a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo.

Informe explicativo al Convenio sobre la ciberdelincuencia

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 quedó 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 racionalizaron 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 avances en el campo de la tecnología de la información influyen directamente en 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, ofrece nuevas posibilidades de muy diversa índole. Estos avances se vieron potenciados por la aparición de las redes y

las superautopistas de la información, con inclusión de Internet, a través de las cuales prácticamente todas las personas pueden tener acceso a cualquier servicio de información electrónica, independientemente del lugar del mundo se encuentre. Al conectarse con los servicios de comunicaciones y de información, los usuarios crean un 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 ejemplo, cuando se cometen a través de Internet, está en conflicto con la territorialidad de las autoridades nacionales encargadas de velar por el cumplimiento de la ley.

9. Por consiguiente, el derecho penal debe mantenerse al corriente de estos avances tecnológicos que brindan 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 las 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, dando curso a su solicitud, 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 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], sobre el derecho sustantivo, y la

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, pág. 106).
2. Véase "La delincuencia informática", Informe del Comité Europeo para los Problemas Criminales, pág. 86.

Recomendación núm. R (95) 13[3], sobre los problemas de derecho procesal en relación con la tecnología de la información.

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

    i. "Examinar, a la luz de las Recomendaciones núm. R (89) 9 sobre la delincuencia relacionada con la informática, y núm. R (95) 13, sobre los problemas de derecho procesal en relación con 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 ejemplo, 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 ejemplo, la interceptación de telecomunicaciones y la vigilancia electrónica de las redes de información, por ejemplo, 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 ejemplo, el cifrado;

    v. la cuestión de la jurisdicción en relación con los delitos relacionados con la tecnología de la información, por ejemplo, la determinación del 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, y

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

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 preparará 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 avances 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 Delegados 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. De conformidad con los términos de referencia originales, el Comité debía finalizar sus labores para el 31 de diciembre de 1999. Dado que, 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 Delegados 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 los esfuerzos desplegados 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 diez 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 Informe 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 Informe 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 de conformidad con el derecho sustantivo penal de cada país y las disposiciones conexas en materia de ciberdelincuencia; 2) establecer, de conformidad con el 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, y 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) Disposiciones 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 la ciberdelincuencia o de los delitos relacionados con el empleo de ordenadores. En primer lugar, define nueve delitos agrupados en cuatro

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 sobre el tráfico; orden de presentación; registro y confiscación de datos informáticos almacenados; obtención en tiempo real de datos sobre el tráfico, e interceptación de datos sobre el 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 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 ciberdelincuencia 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. Además, 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 veinticuatro horas del día los siete 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 de conformidad con el 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, tales como 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 ejemplo, alámbricas o por cable), inalámbricas (por ejemplo, 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 permita el 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 toda entidad pública o privada que brinde a los usuarios de sus servicios 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 ejemplo, 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 sobre el tráfico

28. A los efectos del presente Convenio, los "datos sobre el tráfico" tal como se definen en el párrafo d) del artículo 1, constituyen una categoría separada de datos informáticos que está sujeta 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 sobre el 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 sobre el 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 delicado.

30. La definición enumera de forma exhaustiva las categorías de datos sobre el 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 ejemplo, 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 sobre el 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 conformemente 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 la ciberdelincuencia 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 ejemplo, 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 llevarse a cabo en las leyes nacionales de cada una de las Partes. Se basa en gran medida en las directrices establecidas 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 examinó 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 tal disposición basándose en el derecho a la libertad de expresión. En vista de la complejidad de la cuestión, se decidió que el comité remitiría 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 ciberdelincuencia 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 tanto a las tecnologías actuales como a las futuras.

37. Quienes redactaron el Convenio asumieron que las Partes pueden excluir delitos menores o insignificantes del campo de aplicación de los artículos 2 a 10.

38. Los delitos enumerados tienen una característica particular, a saber, que sus autores deben actuar expresamente de manera ilegítima. La expresión "de manera ilegítima" refleja que el comportamiento descrito no siempre es punible en sí mismo, sino que tal vez sea legal o esté justificado no sólo por excepciones legales clásicas (consentimiento, legítima defensa o necesidad), sino en los casos en que otros principios o intereses excluyen toda responsabilidad penal. La expresión "de manera ilegítima" su significado del contexto en que está utilizada. Así pues, sin restringir la manera en que las Partes pueden aplicar el concepto en su derecho interno, puede referirse a una conducta que no se apoya en ninguna competencia (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 ejemplo, 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 considerarse delitos. Ejemplos específicos de esos tipos de excepciones se presentan en relación con delitos específicos en el texto correspondiente del Informe explicativo *infra*. Queda a criterio de las Partes determinar la manera en que esas exenciones se aplican en sus sistemas jurídicos nacionales (de conformidad con el 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 de conformidad con 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 con respecto a la peligrosidad del comportamiento involucrado o a 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 redactarse 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 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 adelante 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 anteriormente.

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 sobre el 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 ejemplo, 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 proporcionada anteriormente, 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 (por ejemplo, a los fines de efectuar una verificación autorizada o de proteger el sistema informático en cuestión). Por otra parte, no constituye delito acceder a un sistema informático que permita 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 de conformidad con el 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 para 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 ejemplo, 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 oración del artículo 2 suscita controversias. Las controversias provienen de situaciones en que 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 la piratería, de conformidad con la primera oración del artículo 2. Alternativamente, las Partes pueden agregar algunas, o todas, las matizaciones que se enumeran en la segunda oración: 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 de conformidad con el 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 núm. (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, supervisar 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 ejemplo, la Sentencia del Tribunal Europeo 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 ejemplo, 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 ejemplo, 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. En virtud de lo dispuesto en el 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 de conformidad con 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 "dañen" y "deterioren" 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 "borrado" de datos equivale a 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 ejemplo, 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 ejemplo, 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 con arreglo a este artículo. La modificación de los datos sobre el 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 ejemplo, 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 un lenguaje neutral, de tal manera 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 ejemplo, 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 ejemplo, 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 de conformidad con este artículo, aunque cause una obstaculización grave.

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*). A juicio de quienes redactaron este Convenio, dicha 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 ejemplo, 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, de conformidad con su derecho interno.

70. El delito debe cometerse 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 se utilizan indebidamente con el fin de cometer los delitos antedichos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos. Dado que 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 llevar a continuación 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 instrumentos adoptados recientemente 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 en las disposiciones pertinentes en algunos países. Ya se había adoptado un enfoque similar en el Convenio internacional sobre represión de la falsificación de moneda firmado en Ginebra en 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 a poner en línea dispositivos para su utilización por otras personas. Este término abarca también la creación o compilación de hipervínculos para facilitar el acceso a dichos dispositivos. El término "programa informático" incluido en este artículo se refiere a los programas concebidos, por ejemplo, para alterar o incluso destruir datos, o interferir en 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 extensamente 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, aun cuando se produzcan y distribuyan 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 apartado a) del párrafo 1 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 un sistema informático o a una parte del mismo.

75. El apartado b) del párrafo b) establece como delito la posesión de los elementos descritos en los incisos i) o ii) del apartado a) del párrafo 1. En virtud de lo dispuesto en la última oración del apartado b) del párrafo 1, 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 determinar 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 con fines legítimos, por ejemplo, para contrarrestar los ataques a 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". Así pues, 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, sobre la base de 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, tal como lo estipula el inciso ii) del apartado a) del párrafo 1.

Título 2 - Delitos informáticos

79. Los artículos 7 a 10 se refieren a los delitos comunes que suelen cometerse 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 tal vez no abarquen 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 contemplan 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 pretende 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 considerablemente 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 se apoya 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 del contenido 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 da lugar a una situación que corresponde a 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 oración de la disposición permite a las Partes, al aplicar el delito con arreglo a su derecho interno, exigir además que exista 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 en el 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 pertinentes, los elementos constitutivos de la "introducción", "alteración", "borrado" o "supresión" mencionados en el artículo 8.a) se complementan con 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, o la 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 un tercero. 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 que el delito establecido en este artículo comprenda las prácticas comerciales comunes legítimas, destinadas a obtener un beneficio económico, ya que éstas se llevan a cabo legítimamente. Por ejemplo, son legítimas las actividades realizadas en virtud de un contrato válido entre las personas afectadas (por ejemplo, inhabilitar un sitio web, de conformidad con los términos del contrato de que se trate).

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, con el fin de obtener un beneficio económico o de otro tipo para sí o para un tercero. Así, por ejemplo, no se pretende que el delito establecido por este artículo comprenda 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*), aun cuando sean 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 es 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 una función a la hora de apoyar, alentar o facilitar los delitos de índole sexual contra los menores.

94. El apartado a) del párrafo 1 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 b) del párrafo 1 establece como delito la "oferta" de pornografía infantil a través de un sistema informático. El término "oferta" pretende 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" pretende abarcar el hecho de poner en línea pornografía infantil para que sea utilizada por terceros, por ejemplo, mediante la creación de sitios de pornografía infantil. Este párrafo también tiene por objeto 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 apartado c) del párrafo párrafo 1 establece como delito la difusión o la transmisión de pornografía infantil a través de un sistema informático. La "difusión" es la divulgación activa del material. El envío de pornografía infantil a otra persona a través de un sistema informático se consideraría un delito de "transmisión" de pornografía infantil.

97. La expresión "la adquisición, para uno mismo o para terceros" en el apartado d) del párrafo 1 significa obtener activamente pornografía infantil, por ejemplo, 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 apartado e) del párrafo 1. 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 un 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, analgenital 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 apartado a) del párrafo 2 se centra más directamente en la protección contra el abuso de menores. Los apartados b) y c) del párrafo 2 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 apartado b) del párrafo 2, la referencia al término "ilegítimo" podría también permitir, por ejemplo, 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 de edad, de conformidad 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 a la utilización 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 oración 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, de conformidad con los artículos 2 a 8, las Partes están obligadas a tipificar como delito si fueron cometidos de manera "deliberada". Con arreglo 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 basta, por ejemplo, que un proveedor de servicios haya servido de conducto para el material, o albergado un sitio web o una sala de noticias que contuviera dicho material, si no existió la intención exigida de conformidad con el 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 en el momento de la firma o del depósito de los instrumentos de ratificación, aceptación, aprobación o adhesión, en virtud de lo dispuesto en 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 quienes 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 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 abarcan únicamente 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 los 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 Organización Mundial de la Propiedad Intelectual (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 ADPIC, y el Tratado de la 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 tipificadas 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 únicamente 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 a 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 de conformidad con la legislación nacional o con 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 de conformidad con 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 en virtud del 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 a no aplicar el párrafo 2, en su totalidad 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 de conformidad con 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 para 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 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 párrafo 2 del artículo 13, 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 de conformidad con el derecho penal. Con arreglo a las obligaciones impuestas por dichos artículos, esta disposición obliga a las Partes Contratantes a extraer 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 en virtud de 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. Con arreglo a lo dispuesto en el párrafo 3 del artículo 39, nada de lo dispuesto en el Convenio requerirá o invitará a una Parte a establecer facultades o procedimientos distintos de los que figuran en el presente Convenio, ni impedirá 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 la 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, como el registro y la confiscación, sigan siendo eficaces en el volátil entorno tecnológico. Habida cuenta de que 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 sobre el tráfico y la interceptación de los datos sobre el 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 sobre los problemas de derecho procesal 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 recopilación 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 sobre el 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 sobre el 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"), utilizar 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 hacen referencia 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, sólo 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 de conformidad con 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 sean 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. Con la salvedad de 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 pues, 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 con arreglo 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 sobre el 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 del 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 a aplicar las medidas previstas en el artículo 20 (obtención en tiempo real de datos sobre el tráfico) únicamente 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 sobre el tráfico es equivalente a la obtención de datos sobre el 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 sobre el tráfico a la misma serie de delitos a los que se aplican los poderes y procedimientos de interceptación en tiempo real de los datos sobre el contenido. Sin embargo, muchos Estados consideran que la interceptación de los datos sobre el contenido no es equivalente a la obtención de datos sobre el tráfico por lo que respecta a la privacidad y el grado de intrusión, ya que la obtención de los datos sobre el tráfico por sí solos no permite obtener ni revelar el contenido de la comunicación. Como la obtención en tiempo real de los datos sobre el 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 sobre el tráfico.

144. El apartado b) prevé la posibilidad de que las Partes formulen una reserva cuando, a causa de las restricciones que imponga 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 comunicaciones 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 trabajadores de una empresa a los que se brinda la posibilidad de comunicarse entre sí a través de la red informática de la empresa. La expresión "ni 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 emplee las redes públicas de comunicaciones" 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 núms. 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,

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 quedado sin objeto.

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 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 correcta 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 Así pues, se da consideración inicial a la correcta administración de la justicia, los intereses públicos (por ejemplo, la seguridad pública y la salud pública) y otros intereses (por ejemplo, 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

reducción al mínimo 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 ejemplo, los proveedores de servicios. No se aplican a la obtención en tiempo real y a la conservación de los datos sobre el 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 los datos significa guardar para el futuro 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 para el futuro. La retención de los datos es el proceso de almacenar datos. Por el contrario, la conservación de 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 sobre el 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 ejemplo, 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. En algunos Estados existen 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 tiene 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 con arreglo 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 la ciberdelincuencia 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 establecer la identidad de los autores de los delitos. Con el fin de rastrear esas comunicaciones con miras a identificar su origen o destino, es necesario obtener datos sobre el tráfico relacionados con esas comunicaciones pasadas (véase la explicación adicional respecto de la importancia de los datos sobre el 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 ejemplo, los mensajes de correo electrónico, es importante proceder a la conservación de esas comunicaciones con el fin de asegurar que no desaparezcan pruebas esenciales. La obtención de copias de esas comunicaciones pasadas (por ejemplo, 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 pretende abordar esas cuestiones. Por consiguiente, las Partes deberán adoptar las medidas que sean necesarias para la conservación de determinados datos informáticos como medida provisional, durante el tiempo necesario, hasta un máximo de noventa días. Una Parte puede prever la renovación de dicha orden. Esto no significa que los datos se revelan 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 a las autoridades de los datos preservados, 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 u obtener de manera similar 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 otra manera" 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 ejemplo, 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 otra manera" 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 otra manera 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 comprender, por ejemplo, registros comerciales, de salud, personales o de otra índole. Las Partes deben establecer medidas que se utilizarán "en particular cuando existan razones para creer que dichos datos son especialmente 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 se utiliza el dispositivo de almacenamiento 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 sobre el 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 sólo por poco tiempo. Asimismo, la referencia a los "datos sobre el 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 almacenados que se encuentren en poder o bajo el control de esa persona". Así, los datos almacenados pueden realmente estar en poder 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 dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir 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 cual deberán conservarse los datos especificados. El lapso de tiempo debería ser tan largo como sea necesario, hasta un máximo de noventa días, con objeto 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 dicho artículo se especifica que las medidas de conservación adoptadas en respuesta a solicitudes de asistencia mutua "tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, de confiscación u obtención de forma similar, o de 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 a 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 anteriormente , 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 sobre el tráfico (Artículo 17)

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

166. La obtención de los datos sobre el 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 ejemplo, 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, cabe 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 la discusión relativa a la conservación expuesta anteriormente).

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 sobre el 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. Algunas veces los datos sobre el tráfico, o al menos algunos tipos de datos sobre el

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 sobre el 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 sobre el 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. No obstante, 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 sobre el tráfico, a pesar de cualquier obligación que pudiera existir para borrarlos, o imponer la conservación de los correspondientes datos sobre el tráfico. El segundo proveedor de servicios podría notificar de manera similar al siguiente proveedor de servicios de la cadena.

169. Como los datos sobre el 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 sólo 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, deberá revelar con prontitud a las autoridades competentes, o a otra persona designada, un volumen suficiente de datos sobre el tráfico que permita a las autoridades competentes identificar tanto a los proveedores de servicios como el cauce por el cual se transmitió la comunicación. Las autoridades competentes deberían especificar con claridad el tipo de datos sobre el tráfico que deben revelarse. 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 para que ordenen una persona que se encuentre en su territorio que comunique determinados datos informáticos que obren en su poder, o para que ordenen a un proveedor que ofrezca sus servicios en el territorio de dicha Parte que suministre información relativa a los abonados. Los datos en cuestión son los datos almacenados o existentes, y no comprenden aquellos que todavía no se han generado, tales como los datos sobre el tráfico o los datos sobre el 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 más invasivas u 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 dicha 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 sólo es aplicable 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. En virtud de lo dispuesto en el apartado a) del párrafo 1, 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 posea o que se encuentren bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento de datos. La expresión "posea o que se encuentren 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 posea los datos o de que éstos se encuentren bajo su control.

Con arreglo a lo dispuesto en el apartado b) del párrafo 1, las Partes deberán prever también la facultad de ordenar a un proveedor de servicios que ofrezca prestaciones en su territorio que "comunique los datos que posea o que se encuentren bajo su control relativos a los abonados". Al igual que en el apartado a) del párrafo 1, la expresión "que posea o que se encuentren bajo su control"

se refiere a información sobre los abonados que el proveedor de servicios posea físicamente, así como a información sobre los abonados almacenada remotamente que se encuentra bajo el control del proveedor de servicios (por ejemplo, en una instalación remota de almacenamiento de datos provista por otra compañía). La expresión "en conexión con dichos servicios" significa 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 posean ciertas categorías de personas o 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 tales 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, con el 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 utilizarse algunas veces 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 se presente 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 ejemplo, 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 ejemplo, 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, quienes pagan en función del uso que hacen, y quienes los servicios en forma gratuita. También incluye la información sobre 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 ejemplo, móvil), los diferentes servicios conexos utilizados (por ejemplo, desvío de llamadas, buzón de voz, etc.), el número de teléfono u otra dirección técnica (por ejemplo, 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 útiles 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 comprende 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 sobre el 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 se limita a la información directamente relacionada con el uso del servicio de comunicación. También abarca cualquier información, excepto los datos sobre el tráfico o los datos sobre el 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 sobre el tráfico o el 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 únicamente 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 de mantener registros de sus abonados, ni tampoco exige a los proveedores de servicios que se aseguren de la exactitud de dicha información. Así pues, un proveedor de servicios no está obligado a registrar la información sobre 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. Dado que 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 conducir a que se ordene 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, como consecuencia, no pueden obtenerse 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 ejemplo, 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,

con arreglo a lo establecido por 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 está relacionada 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 guardan relación 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, se necesitan 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. Esto obedece a diferentes factores: en primer lugar, los datos se encuentran en forma intangible como, por ejemplo, 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 ejemplo, el disco duro de un ordenador o un disquete) debe confiscarse o secuestrarse, o debe hacerse una copia de los datos, ya sea en forma tangible (por ejemplo, una copia impresa de los datos informáticos) o en forma intangible en un medio físico (por ejemplo, un 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 se revisa, 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 que registren o tengan 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 dispositivo 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 conlleva 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 de datos informáticos que permita almacenar datos informáticos" (apartado b) del párrafo 1 del artículo 19) 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. De conformidad con las leyes de algunas Partes, dicho 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 "registren o tengan acceso de un modo similar". El uso de la palabra tradicional "registrar" indica que el Estado ejerce una facultad coercitiva, y 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, concierne únicamente a medidas que han de adoptarse 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 para 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 para que extiendan 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 para que confisquen u obtengan de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en 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. La prohibición del 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" pretende transmitir que si los datos se suprimen, o si se prohíbe el acceso a los mismos, los datos no se destruyen, sino que siguen existiendo. El sospechoso se encuentra temporalmente privado del acceso a los mismos, pero dicho acceso puede serle restituido al término de las investigaciones o de los procedimientos penales.

199. Así pues, el hecho de confiscar datos, o de obtenerlos de un modo similar, tiene dos funciones: 1) reunir pruebas, por ejemplo, mediante la copia de los datos, o 2) confiscar los datos, por ejemplo, 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 el problema práctico de la dificultad que entraña acceder a los datos que se desea obtener como prueba e identificarlos, en vista del volumen de datos que pueden ser tratados y almacenados, la utilización 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 los mismos, 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 se limitan únicamente a las autoridades que llevan a cabo la investigación. Sin ese tipo de cooperación, dichas 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. Imponer al administrador de un sistema la obligación legal de prestar su ayuda puede también eximir 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 comprender 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 contemplarse 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 sobre el tráfico y la interceptación en tiempo real de los datos sobre el 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 suele estar relacionada 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 las especificidades de sus infraestructuras, son cada vez menos claras 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 se obtienen en el momento en que se produce la comunicación (es decir, "en tiempo real"). Los datos son intangibles en cuanto a su forma (por ejemplo, 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 sobre el tráfico y los datos sobre el contenido. De acuerdo con la definición del artículo 1.d se entiende por "datos sobre el tráfico" cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente. En el Convenio no se define el término "datos sobre el contenido", pero éste se refiere al contenido informativo 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 sobre el tráfico).

210. En muchos Estados se establece una distinción entre la interceptación en tiempo real de datos sobre el contenido y la obtención en tiempo real de datos sobre el 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 sobre el 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 sobre el contenido que a los datos sobre el tráfico. Para contribuir a reconocer la distinción que existe ambas situaciones se obtienen o registran datos, se refiere normativamente en los títulos de los artículos a la obtención de los datos sobre el tráfico como "obtención en tiempo real" y a la obtención de los datos sobre el contenido como "interceptación en tiempo real".

211. En algunos Estados la legislación vigente no establece distinción alguna entre la obtención de datos sobre el tráfico y la interceptación de datos sobre el 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 es muy similar 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 "obtengan o graben" en el texto de ambos artículos 20 y 21.

212. En lo tocante a la interceptación en tiempo real de datos sobre el contenido, en muchos casos la ley establece que la medida sólo es aplicable 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 a tal efecto, 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 sobre el contenido, el artículo 21 dispone específicamente que sólo se requiere que las Partes establezcan esa medida "por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno".

213. Por otro lado, el artículo 20, relativo a la obtención de datos sobre el tráfico, no está sujeto a ese tipo de limitación y, en principio, se aplica a todo delito penal contemplado en el Convenio. Sin embargo, el párrafo 3 del artículo 14 establece que cualquier Parte podrá reservarse el derecho a aplicar la medida exclusivamente a aquellos delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que se aplica la medida de interceptación de los datos sobre el contenido. No obstante, cuando se formule ese tipo de reserva, la Parte deberá considerar limitar esa reserva para permitir la más amplia gama de aplicación de la medida relativa a la obtención de los datos sobre el tráfico.

214. Algunos Estados podrían considerar normalmente que los delitos establecidos en el Convenio no son lo suficientemente graves como para permitir la interceptación de datos sobre el contenido o, en algunos casos, incluso la obtención de datos sobre el tráfico. Sin embargo, dichas técnicas a menudo revisten vital importancia 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 algunas ocasiones no es posible determinar la fuente de la intrusión o la distribución sin obtener en tiempo real datos sobre el tráfico. En ciertos casos, no es posible descubrir la naturaleza de la comunicación sin la interceptación en tiempo real de los datos sobre el 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 sobre el 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 sobre el tráfico con la interceptación de datos sobre el 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 sobre el 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 sobre el contenido y la obtención en tiempo real de los datos sobre el tráfico están sujetas a lo dispuesto en los artículos 14 y 15. Como la interceptación de los datos sobre el 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 sobre el 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 ejemplo, 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]

5. Sentencia del CEDH en el caso de Klass y otros contra Alemania, A28, 06/09/1978.
6. entencia del CEDH en el caso de Kruslin contra Francia, 176-A, 24/04/1990.
7. entencia del CEDH en el caso de Huvig contra Francia, 176-B, 24/04/1990.
8. entencia del CEDH en el caso de Malone contra el Reino Unido, A82, 02/08/1984.
9. entencia del CEDH en el caso de Halford contra el Reino Unido, los informes de 1997 - III, 25/06/1997.

y Lambert[10]). Algunas de estas salvaguardias son aplicables también a la obtención en tiempo real de los datos sobre el tráfico.

Obtención en tiempo real de datos sobre el tráfico (artículo 20)

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

217. Tradicionalmente, la obtención de datos sobre el tráfico respecto de las telecomunicaciones (por ejemplo, las conversaciones telefónicas) ha sido una herramienta de investigación útil para determinar el origen o el destino (por ejemplo, los números de teléfono) y datos conexos (por ejemplo, la hora, la fecha y la duración) de diversos tipos de comunicaciones ilegales (por ejemplo, amenazas, hostigamientos, conspiración, tergiversaciones fraudulentas) y de comunicaciones que aportan pruebas de delitos pasados o futuros (por ejemplo, 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, dado que 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 ejemplo, la pornografía infantil). Del mismo modo, habida cuenta de que 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, dado que 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 ejemplo, la ejecución de programas informáticos), cualquier interferencia en esos datos puede acarrear efectos desastrosos para el buen funcionamiento de los sistemas informáticos. Cuando tienen lugar la distribución ilegal de pornografía infantil, el acceso ilícito a un sistema informático o la interferencia en el buen funcionamiento del sistema informático o la integridad de los datos, especialmente a distancia, como

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

por ejemplo, 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 capacidad para obtener datos sobre el 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 sobre el 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 tal vez sea necesario obtener datos sobre el tráfico respecto de diversas comunicaciones con miras a 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). Sin embargo, deberán especificarse las comunicaciones respecto de las cuales se pueden obtener o registrar datos sobre el tráfico. Así, el Convenio no exige, ni autoriza la vigilancia y obtención generalizada o indiscriminada de grandes volúmenes de datos sobre el 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 apartado a) del párrafo 1, a garantizar que sus autoridades competentes tengan la capacidad para obtener o registrar datos sobre el 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 apartado b) del párrafo 1, las Partes están obligadas a garantizar que sus autoridades competentes están facultadas para obligar a un proveedor de servicios a obtener o grabar datos sobre el tráfico, o a 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 adoptar 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. Dado que ésta es una medida que ha de emprenderse 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 sobre el 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 sobre el 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 apartado b) del párrafo 1 de prestar a las autoridades competentes su colaboración o su asistencia para obtener o grabar los datos sobre el tráfico no tiene sentido si las autoridades competentes no están facultadas para obtener o grabar ellas mismas los datos sobre el 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 apartados a) y b) del párrafo 1, 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 la medidas contempladas en el apartado a) del párrafo 1 "por respeto a los principios establecidos en su ordenamiento jurídico interno", podrá, en su lugar adoptar un enfoque diferente como, por ejemplo, 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 sobre el 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 sobre el contenido, la obtención en tiempo real de datos sobre el 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 para emprender 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), recurrir a la obstrucción del buen funcionamiento 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 ha señalado anteriormente, por lo general se considera que el interés por el respeto de vida privada es menos marcado en lo tocante a la obtención de los datos sobre el tráfico que con respecto a la interceptación de los datos sobre el contenido. Los datos sobre el 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 ejemplo, 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, con arreglo a lo dispuesto en los artículos 14 y 15.

Interceptación de datos sobre el contenido (Artículo 21)

228. Tradicionalmente, la recogida de datos sobre el contenido respecto de las telecomunicaciones (por ejemplo, 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 ejemplo, 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 ejemplo, 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 sobre el contenido de las comunicaciones informáticas es tan, o más, importante como la interceptación en tiempo real de las telecomunicaciones.

229. Por "datos sobre el 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 sobre el tráfico.

230. La mayoría de los elementos de este artículo son idénticos a los del artículo 20. Por lo tanto, los comentarios que figuran anteriormente respecto de la obtención o la grabación de datos sobre el tráfico, la obligación de cooperar y brindar ayuda y las obligaciones de confidencialidad, se aplican igualmente a la interceptación de datos sobre el contenido. Debido al mayor interés por el respeto de la vida privada en el caso de los datos sobre el 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 sobre el contenido pueden ser más rigurosas que las aplicables a la obtención en tiempo real de datos sobre el 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 en virtud de lo dispuesto en los artículos 2 a 11 del presente Convenio.

233. El párrafo a) del párrafo 1 está basado en el principio de territorialidad. Cada Parte tiene la obligación de penalizar 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, aunque el atacante no lo esté.

234. Se contempló 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 involucran 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 apartados a) a c) del párrafo 1 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 del apartado d) del párrafo 1. 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 un 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 apartados b) y c) del párrafo 1 están basados en una variante del principio de territorialidad. Esos apartados 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 apartado a) del párrafo 1 como base para afirmar su jurisdicción. Si el delito se comete a bordo de un buque o una aeronave que se encuentra fuera del territorio del Estado del 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 en el que está registrado el buque o la aeronave puedan también afirmar jurisdicción.

236. El apartado 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. Con arreglo a lo dispuesto en el apartado d), si una persona de una determinada nacionalidad comete un delito en el extranjero, la Parte tiene 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 los, apartados b), c) y d) del párrafo 1. Sin embargo, no se permite ninguna reserva respecto de la afirmación de la jurisdicción territorial reflejada en el apartado 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 párrafo 6 del artículo 24 del presente Convenio.

238. Las bases de la jurisdicción establecidas 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 que se encuentran en numerosos 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 con arreglo al presente párrafo. Por último, la obligación de consulta no es absoluta, sino que ha de tener lugar "siempre que sea oportuno". Así, por ejemplo, si una de las Partes sabe que la consulta no es necesaria (por ejemplo, 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 posponer las consultas, o negarse a efectuarlas.

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. 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 contemplados en los apartados a) y b) del párrafo 2 del artículo 14), 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, como 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 sobre el tráfico) y 34 (Asistencia mutua en relación con la interceptación de datos sobre el 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 aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca, y de su 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 restricción de la utilización), 31 (Asistencia mutua en relación con el acceso a datos informáticos almacenados), 33 (Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico) y 34 (Asistencia mutua relativa a la interceptación de datos sobre el 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 únicamente a los delitos establecidos en los artículos 2 a 11 del Convenio, siempre que estén penalizados en la legislación de las dos Partes implicadas con una pena privativa 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 penalizar algunos de esos delitos con un período máximo de privación de libertad relativamente corto (véase por ejemplo, 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 solicitud 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 del período máximo de privación de libertad que legalmente pudiera ser impuesto por el delito que da lugar a la solicitud de extradición.

246. Al mismo tiempo, de acuerdo con el principio general de que la cooperación internacional en virtud del capítulo III debería estar de conformidad con 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 de conformidad con 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 se considerará que los delitos mencionados en el párrafo 1 figuran entre los delitos que pueden dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes, y que estas últimas se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí. Esto no significa que la extradición deba otorgarse en todas las ocasiones en que se reciba una solicitud, sino más bien que debe existir la posibilidad de conceder la extradición de personas por tales delitos. Con arreglo 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 solicitud formulada respecto de los delitos establecidos con arreglo a este Convenio, podrá aplicar 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 tiene 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 núms. 86 y 98) se aplicarán a las Partes contratantes en dichos acuerdos, y la extradición puede ser denegada 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 solicitud se ha hecho con el fin de perseguir o castigar a una persona por consideraciones de raza, religión, nacionalidad u opiniones políticas).

251. El párrafo 6 se aplica el principio *aut dedere aut judicare* (extraditar o procesar). Dado que muchos Estados deniegan 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 denegada porque el acusado tiene la nacionalidad de la Parte requerida, ésta deberá, a solicitud de la Parte requirente, someter el asunto a sus autoridades competentes para los fines de las actuaciones penales permitentes. Si la Parte cuya solicitud de extradición ha sido denegada 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 ninguna solicitud 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 de emprender 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". Ésta 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 solicitudes 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 de la recepción de solicitudes de extradición o de detención provisional en ausencia de un 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 las solicitudes 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 del depósito por la Parte del 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 concederán asistencia mutua en la mayor medida 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 apartados a) y b) del párrafo 2 del artículo 14), 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. Estos pueden eliminarse pulsando apenas unas teclas o mediante la operación de programas automáticos, lo que hace imposible seguir la pista de un delito hasta su autor o destruye pruebas esenciales de su culpabilidad. Algunas formas de datos informáticos están almacenados únicamente por cortos períodos de tiempo antes de ser eliminados. En otros casos, se puede causar un daño considerable a personas o bienes si las pruebas no se reúnen con rapidez. En esos casos urgentes, no sólo la solicitud, 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 responder a la solicitud de asistencia. El párrafo 3 lo hace 1) facultando a las Partes para que formulen solicitudes 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 solicitudes 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 únicamente 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 utilizarse 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 delicados. 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 prevé el principio de que la asistencia mutua está sujeto a las condiciones previstas en 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 solicitud 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 que se establezca específicamente 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 se ha mencionado 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 contempla en el artículo 27, que siempre ha de aplicarse a la ejecución de las solicitudes 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 denegarse, 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 solicitud implica 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 con arreglo a lo dispuesto en este capítulo. Cuando la Parte requerida se permite exigir la doble tipificación penal como condición para la prestación de asistencia (por ejemplo, cuando la Parte requerida se ha reservado el derecho a 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 de conformidad con las leyes de la Parte requerida, aunque sus leyes ubiquen dicho delito dentro de una categoría diferente de delitos o utilicen una terminología diferente para denominar el delito. Esta disposición se consideró necesaria con el fin de garantizar que las Partes a las que se solicitó 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 con más frecuencia, 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 ninguna solicitud de asistencia mutua. El párrafo 1 faculta al Estado que posee la información para que la transmita a otro Estado sin que medie una solicitud 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 solicitud. 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 debe mantenerse 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 ejemplo, 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 cual tendrá la opción entonces de no proporcionar la información. Sin embargo, si la Parte receptora acepta la condición, deberá 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 sobre la base de 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 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 con arreglo a lo dispuesto en este capítulo se seguirán llevando a cabo con arreglo a lo dispuesto en 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 ejemplo, 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 sobre la base de 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 (párrafo 4 del artículo 25), 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 en el momento de la entrada en vigor del presente Convenio, pero abarca también los instrumentos que pueden adoptarse en el futuro.

264. En los párrafos 2 a 9 del artículo 27 (Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables)

se 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 párrafo 4 del artículo 25 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 o varias autoridades centrales encargadas de enviar y responder a 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 eficaz 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 a la hora de 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 delicadas son tratadas de manera adecuada.

266. Se alienta a las Partes, por motivos de eficacia, a que designen una única autoridad central respecto de la asistencia mutua; por lo general, sería más eficaz que la autoridad designada a tal efecto 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, se tramiten 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 mantenga actualizada.

267. Un objetivo importante de un Estado que solicita asistencia mutua suele ser asegurar que se cumplan las leyes nacionales que rigen la admisibilidad de las pruebas, y que, por consiguiente, las pruebas se puedan utilizar ante sus tribunales. Para cerciorarse de que pueden cumplirse tales requisitos respecto de las pruebas, el párrafo 3 obliga a la Parte requerida que de curso a las solicitudes con arreglo a 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 de conformidad con 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. Aunque la Parte requerida no contemple este requisito en su derecho interno, deberá acceder a la solicitud de la Parte requirente.

268. El párrafo 4 prevé la posibilidad de denegar las solicitudes de solicitudes de asistencia mutua formuladas con arreglo a este artículo. La asistencia podrá denegarse por los motivos previstos en el párrafo 4 del artículo 25 (es decir, los motivos previstos en la legislación de la Parte requerida), incluyendo que la

solicitud pueda atentar contra la soberanía del Estado, su seguridad, el orden público o 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. Con el 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 denegar la solicitud deberían ser pocos y se deberían ejercer con moderación. No deberían ser tan amplios como para dar lugar a que se deniegue categóricamente la asistencia, ni estar sujetos a condiciones onerosas, ni incluir amplias categorías de pruebas o de información.

269. Con arreglo a 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. Dicha 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), el suministro 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 pues, 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 un motivo como tal para denegar asistencia. Antes de invocar "intereses esenciales", como motivo para rechazar la cooperación, la Parte requerida debería en su lugar tratar de establecer condiciones que pudieran permitir la transferencia de los datos. (véase el párrafo 6 del artículo 27 y el párrafo 271 del presente informe).

270. El párrafo 5 permite que la Parte requerida posponga la prestación asistencia, en lugar de denegarla, cuando la adopción de medidas inmediatas respecto de la solicitud pudiera 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 emprender 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, dicha Parte 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 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 comprender cómo ha interpretado la Parte requerida las disposiciones del presente artículo, a establecer una base para realizar consultas, a fin de mejorar la eficiencia futura respecto de la asistencia mutua, y a 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 que 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 hechos y el contenido de la solicitud se mantengan confidenciales. Sin embargo, la confidencialidad no puede exigirse hasta el extremo de socavar la capacidad de la Parte requerida para obtener las pruebas o la información solicitada, por ejemplo, cuando la información deba revelarse 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 la solicitud de confidencialidad, deberá notificar a la Parte requirente, la cual tiene entonces la opción de retirar o modificar su solicitud.

274. Las autoridades centrales designadas con arreglo a lo dispuesto en 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 también debe dirigir una copia de la solicitud efectuada a su propia autoridad central para que sea transmitida a la autoridad central de la Parte requerida. En virtud del apartado b), las solicitudes pueden canalizarse a través de INTERPOL. Las autoridades de la Parte requerida que recibe una solicitud que está fuera de su ámbito de competencia tienen, de conformidad con el apartado c), una doble obligación. En primer lugar, deben 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. Con arreglo al apartado d), las solicitudes podrán transmitirse también directamente, sin la intervención de las autoridades centrales, aunque no sean urgentes, siempre y cuando la autoridad de la Parte requerida pueda dar curso al a solicitud sin recurrir a medidas coercitivas. Por último, el apartado e) permite a una Parte informar a las demás, a través del Secretario General del Consejo de Europa, de que, por razones de eficacia, las solicitudes formuladas deberán dirigirse a la autoridad central.

Confidencialidad y restricción de la utilización (Artículo 28)

275. Esta disposición establece expresamente limitaciones a la utilización de la información o los materiales, con objeto de que la Parte requerida, en los casos en que dicha información o materiales sean particularmente delicados, pueda asegurar que su utilización se limitará al motivo por el cual se concedió la asistencia, o 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 basado en 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 se mantenga confidencial cuando no pueda darse curso a la solicitud ante la ausencia 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 ejemplo, 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 se utilice 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 puedan 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 una de las condiciones impuestas, deberá dar parte de ello a la Parte emisora, que decidirá entonces si facilitará o no la información. Sin embargo, si la Parte receptora está de acuerdo con la condición deberá cumplirla.

280. El párrafo 4 prevé que tal vez sea 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 ejemplo, 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 previsto en el artículo 16 para su uso a nivel nacional. El párrafo 1 de este artículo autoriza a una Parte a formular una solicitud, y el párrafo 3 prevé 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 anteriormente, los datos informáticos son muy volátiles. Basta con pulsar algunas teclas, o con utilizar programas automáticos, para eliminarlos, alterarlos o trasladarlos, para que hagan imposible seguir la pista de un delito hasta su autor, o para que destruyan pruebas esenciales de su culpabilidad. Algunos tipos 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 que garantizara la disponibilidad de dichos datos durante el proceso largo y complejo de la ejecución de una solicitud oficial de asistencia mutua, puede llevar semanas o meses.

283. Esta medida es mucho más rápida que la práctica convencional de asistencia mutua, además de ser 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. Se prefiere 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 éstos sean entregados a los servicios encargados de hacer cumplir la ley en una etapa ulterior. 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 plena revelación de los mismos de conformidad con 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 solicitud 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 prevé 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, desde la perspectiva de la práctica moderna de la asistencia mutua, existe la tendencia a eliminar el requisito de la doble tipificación penal para todas las medidas procesales salvo 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 se limita a conservar 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 la que se solicite la revelación de los datos. En segundo lugar, desde un punto

de vista práctico, 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 antes de establecer dicha existencia. 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 tal vez no comprenda bien hasta mucho más tarde la naturaleza y magnitud del daño. Si la Parte requerida se demora en la conservación de los datos sobre el 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 sólo los conservan algunas horas o días después de efectuada la transmisión. Aunque posteriormente la Parte requirente pudiera establecer la doble tipificación penal, los datos cruciales relativos al tráfico podrían no recuperarse, y el autor del delito nunca se identificaría.

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, el párrafo 4 establece una reserva limitada. 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 a exigir la doble tipificación penal como condición previa para efectuar la conservación de los datos. Con respecto a los delitos establecidos de conformidad con los artículos 2 a 11, se parte del principio de que el requisito de doble incriminación penal se cumple automáticamente, salvo disposiciones contrarias que figuren en las reservas, previstas en el Convenio, que las Partes puedan haber formulado en lo que respecta a las infracciones. Como consecuencia, las Partes pueden imponer esta obligación únicamente 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 denegar 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 u 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 denegar una solicitud de conservación.

288. Algunas veces, la Parte requerida puede caer en la cuenta de que es probable que el custodio de los datos tome medidas que amenacen la confidencialidad, o que socaven la investigación de la Parte requirente (por ejemplo, cuando los datos que se desea conservar están en poder de un proveedor de servicios controlado por un grupo criminal, o de quien es objeto de la investigación propiamente dicha). En tales situaciones, con arreglo a lo dispuesto en el párrafo 6, se deberá informar a la Parte requirente sin demora, de modo que pueda evaluar si corre el riesgo planteado y sigue prosigue 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 este artículo se conservarán al menos durante 60 días mientras esté pendiente el recibo de la solicitud formal de asistencia mutua en la que se pide la revelación de los datos, y seguirán conservándose 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 solicitud de una Parte en la que se cometió un delito, la Parte requerida conservará los datos sobre el tráfico relativos a una transmisión de una comunicación a través de sus ordenadores, con el fin de rastrear la transmisión hasta su origen e identificar al autor del delito, o de localizar pruebas esenciales. Al hacerlo, la Parte requerida puede descubrir que los datos sobre el tráfico localizados en su territorio revelan que la transmisión había sido canalizado 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 sobre el 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 formular una solicitud de rápida conservación y asistencia mutua a ese otro Estado, con el fin de rastrear la transmisión hasta su origen. Si la transmisión ha vuelto al territorio de la Parte requirente, ésta podrá obtener la conservación y la revelación de otros datos sobre el tráfico a través de procesos efectuados a nivel nacional.

291. En virtud de lo dispuesto en el párrafo 2, la Parte requerida podrá negarse a divulgar los datos sobre el tráfico sólo 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 quienes hayan cometido delitos en el ámbito de este Convenio o para localizar pruebas esenciales, los motivos para denegar la revelación deben estar estrictamente limitados, y se acordó excluir la posibilidad de considerar cualquier otro motivo para denegar la asistencia.

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

Asistencia mutua en relación con el acceso a datos informáticos 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 solicitar 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 curso a dicha solicitud lo antes posible cuando 1) existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o modificación, o 2) cuando esos tratados, acuerdos o leyes así lo establezcan.

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

293. Quienes redactaron el Convenio examinaron la cuestión de si una Parte puede acceder de forma unilateral a los datos informáticos almacenados en otra Parte sin solicitar la asistencia mutua. Se analizaron detenidamente 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 acabaron decidiendo que sólo figuraran en el artículo 32 del Convenio las situaciones en las que la acción unilateral se consideraba unánimemente admisible. Acordaron no reglamentar otras situaciones mientras que no se recibieran nuevos datos y prosiguieran las deliberaciones. En este sentido, el párrafo 3 del artículo 39 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 sobre el 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 de cada Parte tengan la capacidad para obtener los datos sobre el tráfico en tiempo real relacionados con las comunicaciones que pasan a través de un sistema informático en otras Partes. Por consiguiente, con arreglo al artículo 33 (Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico), cada Parte

tiene la obligación de recopilar en tiempo real los datos sobre el tráfico para la otra Parte. Si bien este artículo requiere que las Partes cooperen en lo que respecta a estas cuestiones, aquí, como en otros puntos, se da preferencia a las modalidades existentes respecto de la asistencia mutua. Así pues, los términos y condiciones relativos a la concesión de dicha cooperación 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 sobre el tráfico, porque dicha obtención de datos se considera menos intrusiva que la interceptación de datos sobre el contenido o el registro y la confiscación. Sin embargo, una serie de Estados han adoptado un enfoque más restringido. Como consecuencia, de la misma manera que las Partes pueden formular una reserva en virtud de lo dispuesto en el párrafo 3 del artículo 14 (Ámbito de aplicación de las disposiciones sobre procedimiento) 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 sobre el 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, la utilización de la expresión "como mínimo" en el párrafo 2 tiene por objeto 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 sobre el contenido (Artículo 34)

297. Debido al carácter sumamente intrusivo de la interceptación, la obligación de prestar asistencia mutua para la interceptación de los datos sobre el contenido es restringida. La asistencia se facilitará en la medida que lo permitan las leyes y tratados aplicables de las Partes. Dado que 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 sobre 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 se ha indicado anteriormente, combatir de manera eficaz los delitos cometidos mediante el uso de sistemas informáticos y la obtención eficaz de pruebas en formato electrónico exige una respuesta muy rápida. Además, basta con pulsar unas teclas para que pueda tener lugar una acción en una parte del mundo que tenga consecuencias a muchos miles de kilómetros y atravesando muchas franjas horarias. Por esta razón, la cooperación policial existente y las modalidades de asistencia mutua requieren canales complementarios para encarar con éxito los desafíos que plantea la era informática. El canal establecido en el presente artículo se basa en la experiencia obtenida con una red ya operativa, creada bajo los auspicios de las naciones del grupo G8. En virtud de este artículo, cada Parte tiene la obligación de designar un punto de contacto que esté disponible las veinticuatro horas del día y los siete días de la semana con el fin de asegurar la asistencia inmediata en las los apartados a) a c) del párrafo 1 del artículo 35. Se acordó que el establecimiento de esta red es uno de los medios más importantes 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 llevar a cabo directamente, *inter alia*, 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 dentro de su autoridad central encargada de la de asistencia mutua; algunas pueden pensar que la mejor ubicación es en una unidad policial especializada en la lucha contra los delitos informáticos o en 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. Dado que 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 transcurso del tiempo. Al designar el punto de contacto nacional, se debe prestar especial consideración a la necesidad de comunicarse con puntos de contacto 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 figura la capacidad para 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 está integrado en 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, con el fin de que puedan adoptarse 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 para entablar 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 disponer de 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 de los Delegados celebrada en febrero de 1980. Dado que 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 párrafo 1 del artículo 36 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, a saber, Canadá, Japón, Sudáfrica y los Estados Unidos de América, que participaron activamente en la elaboración del Convenio. Una vez que el Convenio entre en vigor, de conformidad con el párrafo 3, podrá invitarse a otros Estados no miembros no cubiertos por esta disposición a adherirse al Convenio, de conformidad con el párrafo 1 del artículo 37.

305. El párrafo 3 del artículo 36 establece en cinco el número de ratificaciones, aceptaciones o aprobaciones requeridas para la entrada en vigor del Convenio. Esa cifra es superior al límite habitual (3) en los tratados del Consejo de Europa, y refleja la convicción de que se necesita un grupo algo más numeroso de Estados para empezar a encarar 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 se ha redactado sobre la base de 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 previa solicitud, 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 supone que si algunas de las Partes se opone a la adhesión del Estado no miembro, el Comité de Ministros en general no lo invitaría a adherirse 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, aunque un Estado no miembro que es Parte planteara una objeción a su adhesión. Esto significa que, en teoría, no suele concederse 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 introducido 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 adherirse al Convenio. Como se ha indicado anteriormente, este requisito es coherente con la práctica, y reconoce que todos los Estados contratantes del Convenio deben poder determinar con qué Estados no miembros van a establecer relaciones convencionales. 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.

Efectos del Convenio (Artículo 39)

307. En los párrafos 1 y 2 del artículo 39 se 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 anteriormente. El enfoque habitual adoptado 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 a los derechos y obligaciones derivados de los convenios multilaterales internacionales existentes relativos 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 de 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 se aborda en el convenio, o han establecido de otro modo sus relaciones respecto de ese tema, estarán facultadas para aplicar dicho acuerdo o tratado o para regular dichas relaciones en consecuencia, en lugar del nuevo convenio, siempre que ello propicie la cooperación internacional.

308. Dado que el Convenio en general tiene la finalidad de complementar, y no de reemplazar, 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 suscitar confusiones innecesarias. En cambio, el párrafo 1 del artículo 39 indica simplemente que el presente Convenio complementa 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 de asistencia judicial 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 conceder prioridad a las normas contenidas en el Convenio. Un ejemplo es el artículo 30, que prevé la rápida revelación de los datos sobre el tráfico conservados cuando sean necesarios para identificar el trayecto de una comunicación específica. En este ámbito específico, el Convenio, como *lex specialis*, debería imponer una norma de primer recurso sobre las disposiciones en los acuerdos de asistencia mutua más generales.

309. Del mismo modo, quienes redactaron el Convenio consideraron que la adopción de un lenguaje que subordinaría la aplicación de los acuerdos en vigor o futuros a la condición de que refuercen o faciliten la cooperación podría plantear problemas, ya que, según el enfoque adoptado en el capítulo sobre

la cooperación internacional, se supone que Partes aplicarán los acuerdos y arreglos internacionales pertinentes.

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

311. 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 párrafo 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 párrafo 2 del artículo 39 reconoce que las Partes son libres de asumir las obligaciones que sean más específicas, además de aquellas ya establecidas en el Convenio, al regular sus relaciones respecto de las materias contempladas 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 ser contrarias a su finalidad.

312. Además, al determinar la relación del Convenio con otros acuerdos internacionales, quienes lo redactaron convinieron que las Partes pueden inspirarse en las disposiciones pertinentes de la Convención de Viena sobre el Derecho de los Tratados.

313. 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 que quedara 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 ejemplo, la Convención de las Naciones Unidas sobre la financiación del terrorismo).

Declaraciones (Artículo 40)

314. 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 pretenden resolver ciertas diferencias conceptuales o jurídicas, lo que tal vez esté más justificado en un tratado de alcance mundial que en el contexto exclusivo del Consejo de Europa. Las declaraciones se consideran interpretaciones aceptables 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 previstas en el Convenio. Puesto que es importante para las Partes en el Convenio saber que elementos adicionales, en su caso, han sido insertados por otras Partes, existe la obligación de declararlos ante el Secretario General del Consejo de Europa en el 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 las Partes tendrán que cumplir la condición de doble tipificación penal al aplicar ciertas facultades procesales. No se estableció ningún límite numérico respecto de las declaraciones.

Cláusula federal (Artículo 41)

315. 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 pretende allanar las dificultades a las que los Estados federales pueden enfrentarse como resultado de la distribución de poderes entre autoridades centrales y regionales. 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 puede haber variaciones

11. Por ejemplo, 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; la Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras, del 10 de junio de 1958, art. 11, y el Convenio para la Protección del Patrimonio Mundial Cultural y Natural, del 16 de noviembre de 1972, art. 34.

menores en la aplicación como resultado de las leyes nacionales y de las prácticas sólidamente establecidas de una Parte que es un Estado federal. Dichas variaciones deben basarse en su Constitución o en otros principios fundamentales 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. Quienes redactaron el Convenio estuvieron de acuerdo en que la aplicación de la cláusula federal sólo conduciría a variaciones menores en la aplicación del Convenio.

316. Por ejemplo, en los Estados Unidos, en virtud de su Constitución y de los principios fundamentales del federalismo, la legislación penal federal suele regular la conductas basándose en sus repercusiones en el comercio interestatal o extranjero, mientras que los asuntos de poca trascendencia o puramente locales están tradicionalmente regulados por los Estados constituyentes. Este enfoque del federalismo aún proporciona una cobertura amplia de las conductas ilícitas contempladas 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 tengan un impacto menor o quesean 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, 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 repercusiones en el comercio interestatal o exterior, 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 de conformidad con lo estipulado en el artículo 41.

317. 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.

318. 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)

319. El artículo 42 prevé una serie de reservas posibles. Este enfoque se deriva de que el Convenio abarca un ámbito del derecho penal y del derecho procesal penal relativamente nuevo para muchos Estados. Además, la naturaleza global del Convenio, que quedará abierto a la firma de los Estados miembros y no miembros del Consejo de Europa, exige que se contemple la posibilidad de hacer dichas reservas. Estas posibilidades de reserva pretenden 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 formular ninguna otra reserva con excepción de las enumeradas. Además, las reservas sólo las puede efectuar una Parte en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, aprobación o adhesión.

320. Reconociendo que para algunas Partes ciertas reservas son esenciales con el fin de 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, éstas deberían retirarse tan pronto como las circunstancias lo permitan.

321. Con objeto de mantener cierta presión sobre las Partes y de lograr que consideren al menos 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 para retirar, posteriormente, las que ya no sean necesarias. Se espera que con el transcurso del tiempo las Partes puedan eliminar tantas reservas como les sea posible a fin de promover la aplicación uniforme del Convenio.

Enmiendas (Artículo 44)

322. 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 estimaron que podrían efectuarse cambios importantes en el Convenio adoptando protocolos adicionales.

323. Las propias Partes pueden examinar la necesidad de incluir enmiendas o protocolos de conformidad con el 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 ayudar a las Partes en sus esfuerzos por modificar o complementar el Convenio.

324. De conformidad con el párrafo 5, cualquier enmienda adoptada entraría en vigor únicamente cuando todas las Partes hayan comunicado su aceptación al Secretario General. Este requisito tiene por objeto garantizar que el Convenio evolucionará de manera uniforme.

Solución de controversias (Artículo 45)

325. El párrafo 1 del artículo 45 establece que el Comité Europeo para los Problemas Criminales (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 hallar una solución pacífica de cualquier controversia concerniente a la interpretación o la aplicación del Convenio. Todo procedimiento de solución de controversias debería ser acordado 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)

326. El artículo 46 crea un marco para que las Partes puedan celebrar consultas respecto de la aplicación del Convenio, el efecto de importantes novedades de carácter tecnológico, jurídico y político relacionadas con la ciberdelincuencia y con 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 a la utilización y aplicación del Convenio, incluidos los efectos de las declaraciones y reservas formuladas en virtud de los artículos 40 y 42.

327. 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 participar 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 ayudar a las Partes en sus respectivos esfuerzos encaminados a completar o modificar el Convenio. Teniendo en cuenta las necesidades de una prevención eficaz y de emprender acciones judiciales eficaces respecto de los delitos informáticos y las cuestiones de privacidad conexas, las posibles repercusiones en 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 el sector privado (véase también el párrafo 14).

328. El párrafo 3 establece del funcionamiento del Convenio después de tres años tras su entrada en vigor, durante los cuales podrán proponerse las enmiendas que se estimen oportunas. El CDPC llevará a cabo dicho examen con la asistencia de las Partes.

329. El párrafo 4 señala que, salvo cuando se haga cargo el Consejo de Europa, las propias Partes deberán financiar todas las consultas que se celebren 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 desplieguen en relación con el Convenio.

Primer protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE núm. 189), Estrasburgo, 28 de enero de 2003

Los Estados miembros del Consejo de Europa y los demás Estados Partes en el Convenio sobre la ciberdelincuencia, abierto a la firma en Budapest el 23 de noviembre de 2001, signatarios del presente Protocolo;

Considerando que la finalidad del Consejo de Europa es realizar una unión más estrecha entre sus miembros;

Recordando que todos los seres humanos nacen libres e iguales en dignidad y derechos;

Haciendo hincapié en la necesidad de garantizar una aplicación plena y efectiva de todos los derechos humanos sin ninguna discriminación ni distinción, tal como se encuentran consagrados en los instrumentos europeos y otros instrumentos internacionales;

Convencidos de que los actos de índole racista y xenófoba constituyen una violación de los derechos humanos y una amenaza contra el Estado de derecho y la estabilidad democrática;

Considerando que el derecho tanto nacional como internacional necesitan dar una respuesta jurídica adecuada a la propaganda de índole racista y xenófoba difundida por medio de los sistemas informáticos;

Conscientes de que la propaganda de esos actos a menudo está penalmente tipificada en las legislaciones nacionales;

Teniendo en cuenta el Convenio sobre la ciberdelincuencia, que establece medios flexibles y modernos de cooperación internacional, y convencidos de la necesidad de armonizar las disposiciones legales sustantivas relativas a la lucha contra la propaganda racista y xenófoba;

Conscientes de que los sistemas informáticos ofrecen un medio sin precedentes para facilitar la libertad de expresión y de comunicación en todo el mundo;

Reconociendo que la libertad de expresión constituye uno de los fundamentos esenciales de una sociedad democrática y que es una de las condiciones básicas para su progreso y para el desarrollo de todo ser humano;

Preocupados, sin embargo, por el riesgo de la mala utilización o de la utilización abusiva de esos sistemas informáticos para difundir propaganda racista y xenófoba;

Conscientes de la necesidad de garantizar un equilibrio idóneo entre la libertad de expresión y una lucha eficaz contra los actos de índole racista y xenófoba;

Reconociendo que el presente Protocolo no pretende menoscabar los principios establecidos en los ordenamientos jurídicos internos acerca de la libertad de expresión;

Teniendo en cuenta los instrumentos jurídicos internacionales pertinentes en este ámbito, y en particular el Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales y su Protocolo nº 12 relativo a la prohibición general de la discriminación, los convenios existentes del Consejo de Europa sobre cooperación en materia penal, en particular el Convenio sobre la ciberdelincuencia, el Convenio internacional sobre la eliminación de todas las formas de discriminación racial de 21 de diciembre de 1965, la Acción común de la Unión Europea de 15 de julio de 1996, adoptada por el Consejo sobre la base del artículo K.3. del Tratado de la Unión Europea, relativa a la acción para luchar contra el racismo y la xenofobia;

Felicitándose de las recientes iniciativas destinadas a promover aún más el entendimiento y la cooperación internacionales en la lucha contra la ciberdelincuencia, el racismo y la xenofobia;

Teniendo en cuenta el Plan de Acción adoptado por los jefes de Estado y de Gobierno del Consejo de Europa con motivo de su II Cumbre (Estrasburgo,

10-11 de octubre de 1997) con el fin de buscar respuestas comunes al desarrollo de las nuevas tecnologías, basadas en las normas y valores del Consejo de Europa;

Han convenido en lo siguiente:

Capítulo I – Disposiciones comunes

Artículo 1 – Finalidad

La finalidad del presente Protocolo es completar, entre las Partes en el Protocolo, las disposiciones del Convenio sobre la ciberdelincuencia, abierto a la firma en Budapest el 23 de noviembre de 2001 (en lo sucesivo denominado "el Convenio"), por lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.

Artículo 2 – Definición

1. A efectos del presente Protocolo:

por *"material racista y xenófobo"* se entenderá todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el calor, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores.

2. Las expresiones y términos empleados en el presente Protocolo se interpretarán de la misma manera que en el Convenio.

Capítulo II – Medidas que deben tomarse a nivel nacional

Artículo 3 – Difusión de material racista y xenófobo mediante sistemas informáticos

1. Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta: difundir o poner a disposición del público de otro modo material racista y xenófobo por medio de un sistema informático.

2. Cualquiera de las Partes podrá reservarse el derecho a no imponer responsabilidad penal a la conducta prevista en el párrafo 1 del presente artículo cuando el material definido en el párrafo 1 del artículo 2 propugne, promueva o incite a una discriminación que no esté asociada con el odio o la violencia, siempre que se disponga de otros recursos eficaces.

3. No obstante lo dispuesto en el párrafo 2 del presente artículo, cualquier Parte podrá reservarse el derecho a no aplicar el párrafo 1 a aquellos casos de discriminación respecto de los cuales, a la luz de los principios establecidos en su ordenamiento jurídico interno en materia de libertad de expresión, no pueda prever los recursos eficaces a que se refiere en dicho párrafo 2.

Artículo 4 – Amenazas con motivación racista y xenófoba

Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta:

amenazar, por medio de un sistema informático, con la comisión de un delito grave, tal como se define en su derecho interno, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o ii) a un grupo de personas que se distinga por alguna de esas características.

Artículo 5 – Insultos con motivación racista y xenófoba

1. Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta

insultar en público, por medio de un sistema informático, i) a personas por razón de su pertenencia a un grupo que se caracterice por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o ii) a un grupo de personas que se distinga por alguna de esas características.

2. Cualquiera de las Partes podrá:

a. exigir que el delito a que se refiere el párrafo 1 del presente artículo tenga como efecto exponer a la persona o grupo de personas previstas en el párrafo 1 al odio, al desprecio o al ridículo, o

b. reservarse el derecho a no aplicar, en su totalidad o en parte, el párrafo 1 del presente artículo.

Artículo 6 – Negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad

1. Cada Parte adoptará las medidas legislativas que sean necesarias para tipificar la siguiente conducta como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho:

difundir o poner a disposición del público de otro modo, por medio de un sistema informático, material que niegue, minimice burdamente, apruebe o justifique actos constitutivos de genocidio o crímenes contra la humanidad, tal como se definen en el derecho internacional y reconocidas como tales por una decisión definitiva y vinculante del Tribunal Militar Internacional, constituido en virtud del Acuerdo de Londres de 8 de agosto de 1945, o de cualquier otro tribunal internacional establecido por los instrumentos internacionales pertinentes y cuya jurisdicción haya sido reconocida por esa Parte.

2. Cualquier de las Partes podrá:

a. exigir que la negación o la minimización burda a que se refiere el párrafo 1 del presente artículo se cometa con la intención de incitar al odio, la discriminación o la violencia contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o

b. reservarse el derecho a no aplicar, en su totalidad o en parte, el párrafo 1 del presente artículo.

Artículo 7 – Cooperación y complicidad

Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometan intencionadamente y sin derecho, la cooperación y la complicidad en la comisión de cualquiera de los delitos tipificados de conformidad con el presente Protocolo, con intención de que se cometa ese delito.

Capítulo III – Relaciones entre el Convenio y el presente Protocolo

Artículo 8 – Relaciones entre el Convenio y el presente Protocolo

1. Los artículos 1, 12, 13, 22, 41, 44, 45 y 46 del Convenio se aplicarán, *mutatis mutandis,* al presente Protocolo.

2. Las Partes harán extensivo el ámbito de aplicación de las medidas definidas en los artículos 14 a 21 y en los artículos 23 a 35 del Convenio a los artículos 2 a 7 del presente Protocolo.

Capítulo IV – Disposiciones finales

1. El presente Protocolo estará abierto a la firma de los Estados signatarios del Convenio, que podrán expresar su consentimiento en quedar vinculados mediante:

a. la firma sin reserva de ratificación, aceptación o aprobación, o

b. la firma sujeta a ratificación, aceptación o aprobación, seguida por la ratificación, aceptación o aprobación.

2. Ningún Estado podrá firmar el presente Protocolo sin reserva de ratificación, aceptación o aprobación, ni depositar un instrumento de ratificación, aceptación o aprobación, a menos que ya haya depositado o deposite simultáneamente un instrumento de ratificación, aceptación o aprobación del Convenio.

3. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General de Consejo de Europa.

Artículo 10 – Entrada en vigor

1. El presente Protocolo entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses después de la fecha en que cinco Estados hayan expresado su consentimiento en quedar obligados por el Protocolo, de conformidad con lo dispuesto en el artículo 9.

2. Respecto de cualquier Estado que exprese posteriormente su consentimiento en quedar vinculado por el Protocolo, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses después de la fecha de su firma sin reserva de ratificación, aceptación o aprobación o del depósito de su instrumento de ratificación, aceptación o aprobación.

Artículo 11 – Adhesión

1. Tras la entrada en vigor del presente Protocolo, todo Estado que se haya adherido al Convenio podrá adherirse también al Protocolo.

2. La adhesión se efectuará mediante el depósito en poder del Secretario General del Consejo de Europa de un instrumento de adhesión que surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses después de la fecha del depósito

Artículo 12 – Reservas y declaraciones

1. Las reservas y declaraciones formuladas por una Parte a una disposición del Convenio serán aplicables igualmente al presente Protocolo, a menos que esa Parte declare lo contrario en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión.

2. Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá declarar, en el momento de la firma

o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la reserva o reservas previstas en los artículos 3, 5 y 6 del presente Protocolo. En el mismo momento, cualquier Parte podrá acogerse, respecto de las disposiciones del presente Protocolo, a la reserva o reservas previstas en el párrafo 2 del artículo 22 y en el párrafo 1 del artículo 41 del Convenio, sin perjuicio de la aplicación hecha por esa Parte en virtud del Convenio. No podrá formularse ninguna otra reserva.

3. Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la posibilidad de exigir elementos adicionales según lo previsto en el párrafo 2.a del artículo 5 y en el párrafo 2.a del artículo 6 del presente Protocolo.

Artículo 13 – Estatuto y retirada de las reservas

1. La Parte que haya formulado una reserva de conformidad con el anterior artículo 12 la retirará, en su totalidad o en parte, tan pronto como las circunstancias lo permitan. Dicha retirada surtirá efecto en la fecha de recepción de una notificación dirigida al Secretario General del Consejo de Europa. Si la notificación declara que la retirada de una reserva debe surtir efecto en la fecha expresada en ella, y dicha fecha es posterior a aquélla en que el Secretario General reciba la notificación, la retirada surtirá efecto en esa fecha posterior.

2. El Secretario General del Consejo de Europa podrá consultar periódicamente a las Partes que hayan formulado una o varias reservas de conformidad con el artículo 12 acerca de las perspectivas de la retirada de esa reserva o reservas.

Artículo 14 – Aplicación territorial

1. Toda Parte podrá designar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el territorio o territorios a que se aplicará el presente Protocolo.

2. En cualquier fecha posterior, toda Parte, mediante declaración dirigida al Secretario General de Consejo de Europa, podrá hacer extensiva la aplicación del presente Protocolo a cualquier otro territorio designado en la declaración. Respecto de dicho territorio, el Protocolo entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses después de la fecha de recepción de la declaración por el Secretario General.

3. Toda declaración formulada al amparo de los dos párrafos anteriores podrá ser retirada, respecto de cualquier territorio designado en esa declaración, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses después de la fecha de recepción de dicha notificación por el Secretario General.

Artículo 15 – Denuncia

1. Toda Parte podrá denunciar en cualquier momento el presente Protocolo mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración del plazo de tres meses después de la fecha de recepción de la notificación por el Secretario General.

Artículo 16 – Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Protocolo así como a cualquier Estado que se haya adherido o haya sido invitado a adherirse al presente Protocolo:

a. toda firma;

b. el depósito de todo instrumento de ratificación, aceptación, aprobación o adhesión;

c. toda fecha de entrada en vigor del presente Protocolo de conformidad con los artículos 9, 10 y 11, y

d. todo otro acto, notificación o comunicación que se refiera al presente Protocolo.

En fe de lo cual, los infrascritos, debidamente autorizados al efecto, firman el presente Protocolo.

Hecho en Estrasburgo, el 28 de enero de 2003, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa transmitirá copias certificadas conformes a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Protocolo y a todo Estado invitado a adherirse al mismo.

Informe explicativo al Primer protocolo adicional

El texto de este Informe explicativo no constituye un instrumento que ofrezca una interpretación autorizada del Protocolo, aunque por su naturaleza tal vez facilite la aplicación de las disposiciones contenidas en el mismo. Este Protocolo se abrió para la firma en Estrasburgo, el 28 de enero de 2003, con motivo de la Primera Parte de la Sesión de 2003 de la Asamblea Parlamentaria.

Introducción

1. Desde la adopción, en 1948, de la Declaración Universal de Derechos Humanos, la comunidad internacional ha logrado importantes avances en la lucha contra el racismo, la discriminación racial, la xenofobia y otras formas relacionadas de intolerancia. Se han establecido leyes nacionales e internacionales, y se han elaborado diversos instrumentos internacionales de derechos humanos. Cabe mencionar, en particular, la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (CERD), adoptada en Nueva York, en 1966, en el marco de las Naciones Unidas. Pese a estos avances, el anhelo de un mundo sin odio ni discriminación racial sigue sin hacerse plenamente realidad.

2. Al mismo tiempo en que los avances tecnológicos, comerciales y económicos acercan a los pueblos del mundo, subsisten en nuestras sociedades la discriminación racial, la xenofobia y otras formas de intolerancia. La globalización trae consigo riesgos que pueden llevar a la exclusión y al aumento de la desigualdad, muy a menudo por motivos raciales y étnicos.

3. En particular, el surgimiento de redes internacionales de comunicación como Internet brinda a ciertas personas medios modernos y poderosos para apoyar el racismo y la xenofobia, y les permite difundir con facilidad y a gran escala expresiones relacionadas. Para poder investigar y procesar a tales personas, la cooperación internacional resulta fundamental. El Convenio sobre la ciberdelincuencia (CETS núm. 185), en lo sucesivo "el Convenio", se redactó con el ánimo de facilitar la asistencia mutua en relación con los delitos informáticos, en el sentido más amplio del término, de una manera flexible y moderna. El propósito de este Protocolo se puede dividir en dos partes: primero, armonizar el derecho penal sustantivo en lo que se refiere a la lucha contra el racismo y la xenofobia en Internet y, segundo, mejorar la cooperación internacional en la materia. Este tipo de armonización facilita la lucha contra tales delitos a nivel nacional e internacional. Si existen correspondencias en la tipificación de los delitos en las legislaciones nacionales, se puede evitar el

abuso de los sistemas informáticos con fines racistas en Partes cuyas normas en este ámbito estén menos bien definidas. 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 ejemplo, respecto de los requisitos de doble tipificación penal.

4. 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 un consenso con respecto a que dichas conductas constituyan 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 de redacción referiría al Comité Europeo para los Problemas Criminales (CDPC) la cuestión de elaborar un Protocolo adicional al Convenio.

5. La Asamblea Parlamentaria, en su Opinión 226(2001) relativa al Convenio, recomendó la creación inmediata de un protocolo adicional al Convenio bajo el título "Ampliación del alcance del Convenio para incluir nuevas formas de delitos", con el propósito de definir y tipificar, entre otros actos, la difusión de propaganda racista.

6. Por consiguiente, el Comité de Ministros confió al Comité Europeo para los Problemas Criminales (CDPC) y, en particular, a su Comité de Expertos relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (PC-RX), la tarea de preparar un proyecto de protocolo adicional, instrumento jurídico vinculante abierto para la firma y ratificación de las Partes del Convenio, que abordase en especial las cuestiones siguientes:

i. la definición y el alcance de los elementos para la tipificación de actos de índole racista y xenófoba cometidos por medio de redes informáticas, inclusive la producción, la oferta, la difusión u otras formas de distribución de materiales o mensajes con contenido semejante a través de redes informáticas, y

ii. el ámbito de aplicación de las disposiciones sustantivas, procesales y de cooperación internacional del Convenio en lo que se refiere a la investigación y enjuiciamiento de los delitos que se definirían en el Protocolo adicional.

7. Este Protocolo representa una ampliación del alcance del Convenio, incluidas sus disposiciones sustantivas, procesales y de cooperación internacional, a fin de abarcar también los delitos de propaganda racista y xenófoba. Así, además de armonizar los elementos de derecho sustantivo con respecto a dichos actos, el Protocolo busca mejorar la capacidad de las Partes para utilizar los medios de cooperación internacional previstos por el Convenio en este ámbito.

Comentario sobre los artículos del Protocolo

Capítulo I – Disposiciones comunes

Artículo 1 – Finalidad

8. La finalidad del presente Protocolo es completar, entre las Partes en el Protocolo, las disposiciones del Convenio por lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.

9. Las disposiciones del Protocolo tienen carácter obligatorio. Con el fin de cumplir estas obligaciones, los Estados Partes no sólo tienen que promulgar las leyes pertinentes sino también garantizar su aplicación efectiva.

Artículo 2 – Definición

Párrafo 1 – "Material racista y xenófobo"

10. A nivel nacional e internacional se han elaborado diversos instrumentos jurídicos para combatir el racismo y la xenofobia. Quienes redactaron este Protocolo tomaron en consideración en particular i) la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (CERD),ii) el Protocolo n.º 12 (STE núm. 177) al Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), iii) la Acción común de 15 de julio de 1996 de la Unión Europea adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la acción contra el racismo y la xenofobia, iv) la Conferencia Mundial contra el Racismo, la Discriminación Racial, la Xenofobia y las Formas Conexas de Intolerancia (Durban, 31 de agosto al 8 de septiembre de 2001), v) las conclusiones de la Conferencia Europea contra el Racismo (Estrasburgo, 13 de octubre de 2000), vi) el estudio completo de la Comisión Europea contra el Racismo y la Intolerancia (ECRI), del Consejo de Europa, publicado en agosto de 2000 (CRI(2000)27), y vii) la Propuesta de la Comisión Europea, de noviembre de

2011, para una Decisión marco del Consejo relativa a la lucha contra el racismo y la xenofobia (en el marco de la Unión Europea).

11. El artículo 10 del CEDH reconoce el derecho a la libertad de expresión, que comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas. De acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos, "el artículo 10 del CEDH es válido no sólo para las informaciones o ideas que son favorablemente recibidas o consideradas como inofensivas o indiferentes, sino también para aquellas que chocan, inquietan u ofenden al Estado o a una fracción cualquiera de la población"[12]. No obstante, el Tribunal estableció que las acciones de los Estados destinadas a restringir el derecho a la libertad de expresión estaban justificadas en virtud de las restricciones del artículo 10, párrafo 2, del CEDH, en particular cuando las ideas o expresiones en cuestión atentan contra los derechos de terceros. Basándose en instrumentos nacionales e internacionales, este Protocolo define en qué medida la difusión de expresiones e ideas racistas y xenófobas atenta contra los derechos de terceros.

12. La definición contenida en el artículo 2 hace referencia a todo material escrito (por ejemplo, textos, libros, revistas, declaraciones, mensajes, etc.), imagen (por ejemplo, imágenes, fotografías, dibujos, etc.) o cualquier otra representación de ideas o teorías, de índole racista o xenófoba, en un formato que pueda ser almacenado, procesado y transmitido por medio de un sistema informático.

13. La definición contenida en el artículo 2 de este Protocolo se refiere ante todo a las conductas que puede generar el material —más que a las expresiones de sentimientos, creencias o aversión que incluya el material. Esta definición se basa, en la mayor medida posible, en definiciones y documentos nacionales e internacionales existentes (ONU, UE).

14. Según la definición, el material debe propugnar, promover o incitar al odio, la discriminación o la violencia. Por "propugnar" se entiende hacer un llamamiento al odio, la discriminación o la violencia; por "promover", fomentar o favorecer estos; por "incitar", impulsar a otros hacia estos.

15. El término "violencia" se refiere al uso ilícito de la fuerza; el término "odio", a la aversión o la enemistad extremas.

---

12. Véase en este contexto, por ejemplo, la sentencia en el caso Handyside de 7 de diciembre de 1976, serie A n.º 24, pág. 23, párrafo 49.

16. Al interpretar el término "discriminación", deben tomarse en consideración el CEDH (artículo 14 y Protocolo 12) y la jurisprudencia pertinente, así como el artículo 1 del CERD. La prohibición de la discriminación contenida en el CEDH garantiza a todos, dentro de la jurisdicción de un Estado Parte, la igualdad en el goce de los derechos y libertades reconocidos en el propio CEDH. El artículo 14 del CEDH contempla una obligación general de los Estados en relación con los derechos y libertades que prevé el CEDH. En este contexto, el término "discriminación" utilizado en el Protocolo se refiere a un trato diferente injustificado que se da a personas o a un grupo de personas sobre la base de determinadas características. En varias sentencias (como la relativa al régimen lingüístico de Bélgica, o la del caso Abdulaziz, Cabales y Balkandali[13]), el Tribunal Europeo de Derechos Humanos señaló que "una diferencia en el trato es discriminatoria si "no tiene una justificación razonable y objetiva", es decir, si no persigue un "propósito legítimo" o no existe una "relación razonable de proporcionalidad entre los medios empleados y el objetivo que se pretende alcanzar". El carácter discriminatorio del trato se debe determinar a la luz de las circunstancias específicas del caso. El artículo 1 de la CERD también puede orientar sobre la interpretación del término "discriminación". Dicha Convención lo define como "toda distinción, exclusión, restricción o preferencia basada en motivos de raza, color, linaje u origen nacional o étnico que tenga por objeto o por resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos humanos y libertades fundamentales en las esferas política, económica, social, cultural o en cualquier otra esfera de la vida pública".

17. El odio, la discriminación o la violencia deben ir dirigidos a personas o grupos de personas por razón de su pertenencia a un grupo caracterizado por "la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores".

18. Cabe señalar que estos motivos no son exactamente los mismos que contempla, por ejemplo, el artículo 1 del Protocolo n.º 12 del CEDH. En efecto, algunos de los motivos contenidos en este último son ajenos a los conceptos de racismo y xenofobia. Los motivos enunciados en el artículo 2 de este Protocolo tampoco son idénticos a los de la CERD en la medida en que ésta

13. Abulaziz, Cabales y Balkandali, sentencia de 28 de mayo de 1985, serie A n.º 94, pág. 32, párrafo 62; caso relativo al régimen jurídico de Bélgica, sentencia de 23 de julio de 1968, serie A n.º 6, pág. 34, párrafo 10.

trata de la "discriminación racial" en general y no del "racismo" como tal. En general, estos motivos han de interpretarse en el sentido que les confieren la práctica y las leyes nacionales e internacionales. No obstante, algunos de ellos exigen una explicación más detallada en cuanto a su sentido específico en el contexto de este Protocolo.

19. El término "ascendencia" se refiere principalmente a personas o grupos de personas cuyos ascendientes podrían ser identificados por ciertas características (como la raza o el color), aunque tales características no necesariamente existan todavía. Pese a esto, debido a su ascendencia, tales personas o grupos de personas pueden ser objeto de odio, discriminación o violencia. La "ascendencia" no está relacionada con el origen social.

20. La noción de "origen nacional" ha de entenderse en un sentido amplio basado en los hechos. Ésta puede referirse a la historia de las personas, no sólo en relación con la nacionalidad o el origen de sus ancestros, sino también con su propia pertenencia nacional, independientemente de que aún posean o no determinada nacionalidad desde el punto de vista jurídico. Cuando una persona tiene más de una nacionalidad o es apátrida, la interpretación amplia de esta noción tiene el propósito de protegerla si es víctima de discriminación por cualquiera de estos motivos. Además, la noción de "origen nacional" puede referirse al hecho de pertenecer no sólo a uno de los países que son reconocidos como tales por la comunidad internacional, sino también a minorías u otros grupos de personas, con características similares.

21. La noción de "religión" suele estar contemplada en las legislaciones nacionales y en los instrumentos internacionales. Esta tiene que ver con la convicción y las creencias. Como tal, incluirla en la definición acarrearía el riesgo de ir más allá del ámbito de aplicación de este Protocolo. Ahora bien, la religión puede ser utilizada como pretexto, excusa o sustituto de otros factores enumerados en la definición. Por lo tanto, el término "religión" debe interpretarse en este sentido estricto.

Párrafo 2

22. Al prever que las expresiones y términos empleados en el Protocolo se interpreten de la misma manera que en el Convenio, este artículo garantiza una interpretación uniforme de ambos textos. De conformidad con lo anterior, los términos y expresiones empleados en este Informe explicativo deberán interpretarse del mismo modo en que se interpretan los del Informe explicativo del Convenio.

Capítulo II – Medidas que deben tomarse a nivel nacional

Consideraciones generales

23. Los delitos previstos en este Protocolo contienen una serie de elementos comunes tomados del Convenio. A efectos de claridad, los párrafos conexos del Informe explicativo del Convenio se incluyen a continuación.

24. 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 (por ejemplo, a efectos del cumplimiento de la ley, con fines académicos o con propósitos de investigación). El término "ilegítimo" deriva su significado del contexto en que es 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 Protocolo no afecta a las conductas legítimas de un gobierno (por ejemplo, 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. Queda a criterio de las Partes determinar la manera en que esas exenciones son implementadas en sus sistemas jurídicos nacionales (de conformidad con el derecho penal o de algún otro modo).

25. Todos los delitos contenidos en el Protocolo deben ser cometidos de manera "deliberada" para que se aplique la responsabilidad penal. En ciertos casos, un elemento deliberado específico forma parte del delito. Los redactores del Protocolo, al igual que los del Convenio, convinieron en que el significado exacto del término "deliberado" debería ser interpretado de conformidad con las leyes de cada país. Una persona no puede ser considerada responsable penalmente por ninguno de los delitos previstos en este Protocolo si no se cumple el requisito de que haya actuado de modo deliberado. 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 con arreglo 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.

26. En cuanto a la noción de "sistema informático", es la misma que se emplea en el Convenio y que se explica en los párrafos 23 y 24 de su Informe explicativo. Esto constituye una aplicación del artículo 2 de este Protocolo (véase también la explicación del artículo 2 proporcionada anteriormente).

Artículo 3 – Difusión de material racista y xenófobo mediante sistemas informáticos

27. Este artículo exige que los Estados Partes tipifiquen como delito el acto de difundir o poner a disposición del público de otro modo, por medio de un sistema informático, material racista y xenófobo. El acto de difundir o poner a disposición es de índole delictiva únicamente si la intención también se refiere al carácter racista y xenófobo del material.

28. Por "difundir" se entiende la distribución activa a terceros de material racista y xenófobo, como se define en el artículo 2 del Protocolo, mientras que por "poner a disposición" se hace referencia a poner en línea material racista y xenófobo para que sea utilizado por terceros. Este término también busca cubrir la creación o la compilación de hipervínculos destinada a facilitar el acceso a este material.

29. El término "del público" utilizado en el artículo 3 deja en claro que los mensajes o expresiones de carácter privado que sean comunicados o transmitidos mediante un sistema informático no entran en el ámbito de aplicación de esta disposición. En efecto, al igual que las formas tradicionales de correspondencia, tales comunicaciones o expresiones están protegidas por el artículo 8 del CEDH.

30. Para determinar si una comunicación de material racista y xenófobo es de carácter privado o si constituye una difusión al público, deberán tenerse en cuenta las circunstancias del caso. El criterio principal es la intención del remitente en el sentido de que el mensaje llegue únicamente a un destinatario determinado. La existencia de esta intención subjetiva se puede definir teniendo en cuenta una serie de factores objetivos, como el contenido del mensaje, la tecnología utilizada, las medidas de seguridad aplicadas y el contexto en el que se envía el mensaje. El hecho de que los mensajes sean enviados al mismo tiempo a más de un destinatario, el número de receptores

y la naturaleza de la relación entre el remitente y el receptor o receptores, son factores que ayudan a determinar si una comunicación puede considerarse privada.

31. El intercambio de material racista y xenófobo en salas de chat o la publicación de mensajes similares en grupos de noticias o foros de discusión son ejemplos de puesta a disposición al público. En estos casos, el material es accesible para cualquier persona. Incluso cuando el acceso al material requiera autorización mediante una contraseña, se considerará que el material es accesible al público en los casos en que dicha autorización sea otorgada a cualquier persona o a toda persona que cumpla ciertos criterios. A fin de determinar si la difusión o puesta a disposición estaba destinada al público, se debe tener en cuenta la naturaleza de la relación entre las personas en cuestión.

32. Los párrafos 2 y 3 tienen la finalidad de permitir una reserva en circunstancias muy limitadas. Se deben leer de manera conjunta y secuencial. Así, cualquiera de las Partes podrá, en primer lugar, reservarse el derecho a no imponer responsabilidad penal a la conducta prevista en este artículo cuando el material propugne, promueva o incite a una discriminación que no esté asociada con el odio o la violencia, siempre que se disponga de otros recursos eficaces. Estos recursos pueden ser, por ejemplo, civiles o administrativos. Cuando, a la luz de los principios establecidos en su ordenamiento jurídico interno en materia de libertad de expresión, alguna de las Partes no pueda prever estos recursos eficaces, podrá reservarse el derecho a no aplicar la obligación del párrafo 1 de este artículo, si esta se refiere únicamente al acto de propugnar, promover o incitar a una discriminación que no esté asociada con el odio o la violencia. Una Parte puede restringir aún más el ámbito de aplicación de la reserva al exigir que la discriminación sea, por ejemplo, insultante, degradante o amenazante para un grupo de personas.

Artículo 4 – Amenazas con motivación racista y xenófoba

33. La mayoría de las legislaciones prevén la penalización de los actos de amenaza en general. Los redactores acordaron poner de relieve en el Protocolo que las amenazas por motivos racistas y xenófobos deben, sin lugar a dudas, ser penalizadas.

34. La noción de "amenaza" puede referirse a una advertencia que cause temor a las personas a las que está dirigida, en el sentido de verse afectadas por la comisión de un delito grave (por ejemplo, en relación con la vida, con la seguridad o la integridad personal, con daños a los bienes, etc., de la víctima

o de sus familiares). Los Estados Parte pueden determinar libremente cuáles son los delitos graves.

35. Según este artículo, la amenaza debe estar dirigida i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o ii) a un grupo de personas que se distinga por alguna de esas características. La amenaza no necesariamente debe ser pública. Este artículo cubre también las amenazas mediante comunicaciones privadas.

Artículo 5 – Insultos con motivación racista y xenófoba

36. El artículo 5 trata de los insultos en público a una persona o a un grupo de personas por razón de su pertenencia o supuesta pertenencia a un grupo que se distinga por características específicas. La noción de "insulto" se refiere a toda expresión ofensiva, despectiva o insultante que afecte al honor o la dignidad de una persona. Por la expresión en sí misma debe resultar claro que el insulto está directamente relacionado con la pertenencia de la persona insultada a un grupo. A diferencia de lo que ocurre con la amenaza, esta disposición no cubre los insultos expresados en comunicaciones privadas.

37. El inciso i) del párrafo 2 permite a las Partes exigir que la conducta también tenga como efecto exponer a la persona o grupo de personas al odio, al desprecio o al ridículo, no sólo de manera potencial sino también real.

38. El inciso ii) del párrafo 2 permite a las Partes emitir reservas más amplias, incluso a efectos de excluir la aplicación del párrafo 1.

Artículo 6 – Negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad

39. En los últimos años, los tribunales nacionales han tratado varios casos en los que ciertas personas han expresado ideas o teorías (en público, en los medios, etc.) con el objetivo de negar, minimizar burdamente, aprobar o justificar los graves crímenes cometidos durante la Segunda Guerra Mundial (en particular el Holocausto).Estos comportamientos utilizan a menudo el pretexto de la investigación científica, cuando en realidad apuntan a apoyar y promover la motivación política que dio lugar al holocausto. Además, dichos comportamientos han inspirado —o incluso estimulado y animado— a grupos racistas y xenófobos en su acción, que puede incluir el uso de sistemas informáticos. La expresión de tales ideas es un insulto a (la memoria de) aquellas personas

que han sido víctimas de estos hechos funestos, así como a sus familiares. Por lo demás, atenta contra la dignidad de la comunidad humana.

40. El artículo 6, que tiene una estructura similar a la del artículo 3, aborda este problema. Los redactores convinieron en que era importante tipificar como delito las conductas relacionadas con expresiones que nieguen, minimicen burdamente, aprueben o justifiquen actos constitutivos de genocidio o crímenes contra la humanidad, tal como se definen en el derecho internacional y reconocidas como tales por una decisión definitiva y vinculante del Tribunal Militar Internacional, constituido en virtud del Acuerdo de Londres de 8 de agosto de 1945. Esto se debe a que las conductas más importantes y establecidas que habían dado lugar a genocidio y crímenes contra la humanidad ocurrieron durante el período comprendido entre 1940 y 1945. No obstante, los redactores reconocieron que desde entonces han ocurrido otros casos de genocidio y crímenes contra la humanidad, que estuvieron fuertemente motivados por teorías e ideas de índole racista y xenófoba. Por lo tanto, consideraron necesario no limitar el alcance de esta disposición únicamente a los crímenes cometidos por el régimen nazi durante la Segunda Guerra Mundial y establecidos como tales por el Tribunal de Nuremberg, sino extenderlo también a los genocidios y crímenes contra la humanidad establecidos por otros tribunales internacionales creados desde 1945 mediante los instrumentos jurídicos internacionales pertinentes (por ejemplo, resoluciones del Consejo de Seguridad de las Naciones Unidas, tratados multilaterales, etc.). Estos tribunales pueden ser, por ejemplo, los Tribunales Penales Internacionales para la antigua Yugoslavia, para Rwanda, el Tribunal Penal Internacional. Este artículo permite referirse a decisiones finales y vinculantes de futuros tribunales internacionales, en la medida en que la jurisdicción de dichos tribunales sea reconocida por el Estado Parte en este Protocolo.

41. La disposición busca dejar en claro que los hechos cuya exactitud histórica haya sido establecida no pueden ser negados, minimizados burdamente, aprobados o justificados con vistas a respaldar estas teorías e ideas aborrecibles.

42. El Tribunal Europeo de Derechos Humanos ha aclarado que la negación o revisión de "hechos históricos claramente establecidos, como el Holocausto, […] quedaría sustraída por el artículo 17 a la protección del artículo 10" del CEDH (véase en este contexto la sentencia Lehideux e Isorni, de 23 de septiembre de 1998)[14].

14. Sentencia en el caso Lehideux e Isorni de 23 de septiembre de 1998, Informes 1998-VII, párrafo 47.

43. El párrafo 2 del artículo 6 permite a cualquiera de las Partes i) exigir, a través de una declaración, que la negación o la minimización burda a que se refiere el párrafo 1 del artículo 6 se cometa con la intención de incitar al odio, la discriminación o la violencia contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o bien ii) reservarse el derecho a no aplicar, en su totalidad o en parte, esta disposición.

Artículo 7 – Cooperación y complicidad

44. El propósito de este artículo es tipificar como delito la cooperación y la complicidad en la comisión de cualquiera de los actos delictivos previstos en los artículos 3 a 6. Contrariamente al Convenio, el Protocolo no contempla la tipificación de las tentativas de comisión de los delitos en él previstos, en la medida en que muchas de las conductas tipificadas tienen una naturaleza preparatoria.

45. La responsabilidad por cooperación o complicidad surge cuando el autor de un delito previsto en el Protocolo actúa con la colaboración de otra persona que también tiene la intención de que se cometa el delito. Por ejemplo, si bien la transmisión de material racista y xenófobo a través de Internet supone la participación de proveedores de servicio que sirvan como conducto, no será responsable en virtud de esta sección un proveedor que no tenga intención delictiva. Así, un proveedor de servicios no está obligado a vigilar activamente el contenido para evitar una responsabilidad penal de conformidad con esta disposición.

46. Como ocurre con todos los delitos establecidos de conformidad con el Protocolo, la cooperación y la complicidad deben tener un carácter intencional.

Capítulo III – Relaciones entre el Convenio y el presente Protocolo

Artículo 8 – Relaciones entre el Convenio y el presente Protocolo

47. El artículo 8 trata de la relación entre el Convenio y este Protocolo, y evita incluir en el segundo una serie de disposiciones del primero. Así, indica que algunas de las disposiciones del Convenio se aplicarán, *mutatis mutandis*, al Protocolo (por ejemplo, en lo referente a formas de responsabilidad y sanción, competencia y una parte de las disposiciones finales). El párrafo 2 recuerda a las Partes que las medidas definidas en el Convenio deberían aplicarse a los delitos previstos en este Protocolo. Con fines de claridad, se especifican los artículos pertinentes.

Capítulo IV – Disposiciones finales

48. Las disposiciones contenidas en este capítulo se basan, en su mayoría, en 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 9 al 16 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" (véanse también en este contexto los párrafos 304-330 del Informe explicativo del Convenio).

49. El párrafo 2 del artículo 12 especifica que las Partes podrán formular las reservas definidas en los artículos 3, 5 y 6 de este Protocolo. No podrá formularse ninguna otra reserva.

50. Este Protocolo se abre a la firma únicamente de los signatarios del Convenio. El Protocolo entrará en vigor tres meses después de que cinco Partes en el Convenio hayan expresado su consentimiento en quedar obligados por el Protocolo (artículos 9 y 10).

51. El Convenio permite reservas con respecto a ciertas disposiciones que, a través de la cláusula de relación del artículo 8 del Protocolo, también puedan tener un impacto sobre las obligaciones de una Parte en virtud del Protocolo. No obstante, cualquier Parte puede notificar al Secretario General que no aplicará esta reserva respecto al contenido del Protocolo. Esto se expresa en el artículo 12, párrafo 2, del Protocolo.

52. Sin embargo, cuando alguna de las Partes no haya hecho uso de esta posibilidad de reserva en virtud del Convenio, puede tener la necesidad de restringir sus obligaciones en relación con los delitos previstos en el Protocolo. El párrafo 2 del artículo 12 permite a las Partes hacer esto en relación con el párrafo 2 del artículo 22 y el párrafo 1 del artículo 41 del Convenio.

Segundo Protocolo adicional relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas (STCE núm. 224) Estrasburgo, 12 de mayo de 2022

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados Partes en el Convenio sobre la Ciberdelincuencia (STE nº 185, en adelante "el Convenio"), abierto a la firma en Budapest el 23 de noviembre de 2001, firman el presente,

Teniendo en cuenta el alcance y el impacto del Convenio en todas las regiones del mundo;

Recordando que el Convenio ya está complementado por el Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE nº 189), abierto a la firma en Estrasburgo el 28 de enero de 2003 (en adelante, "el Primer Protocolo"), entre las Partes en dicho Protocolo;

Teniendo en cuenta los tratados vigentes del Consejo de Europa sobre cooperación en materia penal, así como otros acuerdos y convenios sobre cooperación en materia penal entre las Partes en el Convenio;

Teniendo en cuenta también el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), modificado por su Protocolo de enmienda (STCE nº 223), abierto a la firma en Estrasburgo el 10 de octubre de 2018, y al que cualquier Estado puede ser invitado a adherirse;

Reconociendo el creciente uso de las tecnologías de la información y la comunicación, incluidos los servicios de internet, y el aumento de la ciberdelincuencia, que constituye una amenaza para la democracia y el Estado de Derecho, y que muchos Estados consideran también una amenaza para los derechos humanos;

Reconociendo también el creciente número de víctimas de la ciberdelincuencia y la importancia de obtener justicia para esas víctimas;

Recordando que los gobiernos tienen la responsabilidad de proteger a la sociedad y a las personas contra la delincuencia, no sólo fuera de la red sino también en línea, incluso mediante investigaciones y procesamientos penales eficaces;

Conscientes de que las pruebas de cualquier delito penal se almacenan cada vez más en forma electrónica en sistemas informáticos de jurisdicciones extranjeras, múltiples o desconocidas, y convencidos de que se necesitan medidas adicionales para obtener legalmente dichas pruebas a fin de permitir una respuesta eficaz de la justicia penal y defender el Estado de Derecho;

Reconociendo la necesidad de una mayor y más eficaz cooperación entre los Estados y el sector privado, y que en este contexto es necesaria una mayor claridad o seguridad jurídica para los proveedores de servicios y otras entidades en relación con las circunstancias en que pueden responder a las solicitudes directas de las autoridades de justicia penal de otras Partes para la divulgación de datos electrónicos;

Por consiguiente, con el fin de seguir reforzando la cooperación en materia de ciberdelincuencia y la obtención de pruebas en forma electrónica de cualquier delito penal a efectos de investigaciones o procedimientos penales específicos mediante instrumentos adicionales relativos a una asistencia mutua más eficaz y otras formas de cooperación entre las autoridades competentes; la cooperación en situaciones de emergencia, y la cooperación directa entre las autoridades competentes y los proveedores de servicios y otras entidades que posean o controlen la información pertinente;

Convencidos de que la cooperación transfronteriza eficaz a efectos de la justicia penal, incluso entre los sectores público y privado, se beneficia de condiciones y salvaguardias eficaces para la protección de los derechos humanos y las libertades fundamentales;

Reconociendo que la recogida de pruebas electrónicas para las investigaciones penales a menudo afecta a datos personales, y reconociendo el requisito de

muchas Partes de proteger la intimidad y los datos personales para cumplir sus obligaciones constitucionales e internacionales, y

Conscientes de la necesidad de garantizar que las medidas efectivas de la justicia penal en materia de ciberdelincuencia y la recogida de pruebas en forma electrónica estén sujetas a condiciones y salvaguardias que prevean la adecuada protección de los derechos humanos y las libertades fundamentales, incluidos los derechos derivados de las obligaciones que los Estados han contraído en virtud de los instrumentos internacionales de derechos humanos aplicables, como el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 (STE nº 5) del Consejo de Europa, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966, la Carta Africana sobre los Derechos Humanos y de los Pueblos de 1981, la Convención Americana sobre Derechos Humanos de 1969 y otros tratados internacionales de derechos humanos,

Han acordado lo siguiente:

Capítulo I - Disposiciones comunes

Artículo 1 - Finalidad

El propósito del presente Protocolo es complementar:

a. el Convenio entre las Partes en el presente Protocolo, y

b. el Primer Protocolo entre las Partes en el presente Protocolo que son también Partes en el Primer Protocolo.

Artículo 2 - Ámbito de aplicación

1. Salvo que se especifique lo contrario en el presente Protocolo, las medidas descritas en el presente Protocolo se aplicarán:

a. entre las Partes en el Convenio que sean Partes en el presente Protocolo, a las investigaciones o procedimientos penales específicos relativos a los delitos relacionados con sistemas y datos informáticos, y a la obtención de pruebas en forma electrónica de un delito penal, y

b. en lo que respecta a las Partes en el Primer Protocolo que sean Partes en el presente Protocolo, a investigaciones o procedimientos penales específicos relativos a delitos penales tipificados con arreglo al Primer Protocolo.

2. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para cumplir las obligaciones establecidas en el presente Protocolo.

Artículo 3 - Definiciones

1. Las definiciones que figuran en el artículo 1 y en el párrafo 3 del artículo 18 del Convenio se aplican al presente Protocolo.

2. A los efectos del presente Protocolo, se aplicarán las siguientes definiciones adicionales:

a. por "autoridad central" se entenderá la autoridad o autoridades designadas en virtud de un tratado o acuerdo de asistencia mutua sobre la base de la legislación uniforme o recíproca en vigor entre las Partes interesadas o, en su defecto, la autoridad o autoridades designadas por una Parte en virtud del párrafo 2.a del artículo 27 del Convenio;

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

c. por "emergencia" se entenderá una situación en la que existe un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física;

d. por "datos personales" se entenderá información relativa a una persona física identificada o identificable, y

e. por "Parte transferente" se entenderá la Parte que transmite los datos en respuesta a una solicitud o como parte de un equipo conjunto de investigación, o a efectos de la sección 2 del capítulo II, la Parte en cuyo territorio se encuentra un proveedor de servicios transmisor o una entidad que proporciona servicios de nombres de dominio.

Artículo 4 - Lengua

1. Las solicitudes, las órdenes y la información adjunta presentadas a una Parte estarán redactadas en una lengua aceptable para la Parte requerida o para la Parte notificada en virtud del párrafo 5 del artículo 7, o irán acompañadas de una traducción a dicha lengua.

2. Las órdenes en virtud del artículo 7 y las solicitudes en virtud del artículo 6, así como cualquier información que las acompañe, deberán:

a. presentarse en una lengua de la otra Parte en la que el proveedor de servicios o la entidad acepte un proceso

b. presentarse en otra lengua aceptable para el proveedor de servicios o la entidad, o

c. ir acompañadas de una traducción a una de las lenguas previstas en los párrafos 2.a o 2.b.

Capítulo II - Medidas de cooperación reforzada

Sección 1 - Principios generales aplicables al capítulo II

Artículo 5 - Principios generales aplicables al capítulo II

1. Las Partes cooperarán, de conformidad con las disposiciones de este capítulo, en la mayor medida posible.

2. La sección 2 de este capítulo se compone de los artículos 6 y 7. Establece procedimientos para mejorar la cooperación directa con proveedores y entidades en el territorio de otra Parte. La sección 2 se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua sobre la base de una legislación uniforme o recíproca en vigor entre las Partes interesadas.

3. La sección 3 de este capítulo se compone de los artículos 8 y 9. Establece procedimientos para mejorar la cooperación internacional entre las autoridades para la divulgación de los datos informáticos almacenados. La sección 3 se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua sobre la base de una legislación uniforme o recíproca en vigor entre las Partes requirente y requerida.

4. La sección 4 de este capítulo consiste en el artículo 10. Prevé los procedimientos relativos a la asistencia mutua de emergencia. La sección 4 se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua sobre la base de una legislación uniforme o recíproca en vigor entre las Partes requirente y requerida.

5. La sección 5 de este capítulo se compone de los artículos 11 y 12. La sección 5 se aplicará cuando no exista un tratado o acuerdo de asistencia mutua basado en una legislación uniforme o recíproca en vigor entre las Partes requirente y requerida. Las disposiciones de la sección 5 no se aplicarán cuando exista dicho tratado o acuerdo, salvo lo dispuesto en el párrafo 7 del artículo 12. No obstante, las Partes interesadas podrán decidir de común

acuerdo aplicar las disposiciones de la sección 5 en lugar de las mismas, si el tratado o acuerdo no lo prohíbe.

6. Cuando, de conformidad con las disposiciones del presente Protocolo, se permita a la Parte requerida condicionar la cooperación a la existencia de doble incriminación, se considerará cumplida esta condición, independientemente de que su legislación incluya el delito en la misma categoría de delitos o lo denomine con la misma terminología que la Parte requirente, si la conducta constitutiva del delito para el que se solicita la asistencia es un delito penal en virtud de su legislación.

7. Las disposiciones de este capítulo no restringen la cooperación entre las Partes, o entre las Partes y los proveedores de servicios u otras entidades, a través de otros acuerdos, convenios, prácticas o legislación nacional aplicables.

Sección 2 - Procedimientos para mejorar la cooperación directa con proveedores y entidades de otras Partes

Artículo 6 - Solicitud de información sobre el registro de nombres de dominio

1. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes, a efectos de investigaciones o procedimientos penales específicos, para emitir una solicitud a una entidad que preste servicios de registro de nombres de dominio en el territorio de otra Parte para obtener la información que esté en posesión o bajo el control de la entidad, con el fin de identificar o ponerse en contacto con el titular de un nombre de dominio.

2. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para permitir que una entidad en su territorio divulgue dicha información en respuesta a una solicitud en virtud del párrafo 1, sujeto a las condiciones razonables previstas en la legislación nacional.

3. La solicitud en virtud del párrafo 1 deberá incluir:

a. la fecha de emisión de la solicitud, y la identidad y los datos de contacto de la autoridad competente que emite la solicitud;

b. el nombre de dominio sobre el que se solicita información y una lista detallada de la información solicitada, incluidos los elementos de datos concretos;

c. una declaración en la que se indique que la solicitud se emite en virtud del presente Protocolo, que la necesidad de la información se debe a su pertinencia para una investigación o procedimiento penal específico y que la información sólo se utilizará para esa investigación o procedimiento penal específico, y

d. el periodo de tiempo y la forma en que se divulgará la información y cualquier otra instrucción especial de procedimiento.

4. Si es aceptable para la entidad, una Parte podrá presentar una solicitud en virtud del párrafo 1 en formato electrónico. Es posible que se requieran niveles adecuados de seguridad y autentificación.

5. En caso de falta de cooperación por parte de una entidad descrita en el párrafo 1, la Parte requirente podrá pedir a la entidad que explique la razón por la que no divulga la información solicitada. La Parte requirente podrá solicitar consultas con la Parte en la que se encuentre la entidad, con miras a determinar las medidas disponibles para obtener la información.

6. Cada Parte, en el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, o en cualquier otro momento, comunicará al Secretario General del Consejo de Europa la autoridad designada para los fines de consulta en virtud del párrafo 5.

7. El Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de las autoridades designadas por las Partes con arreglo al párrafo 6. Cada Parte se asegurará de que los datos que haya facilitado para el registro sean correctos en todo momento.

Artículo 7 - Divulgación de la información de los abonados

1. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para emitir una orden que se presentará directamente a un proveedor de servicios en el territorio de otra Parte, a fin de obtener la divulgación de información especificada y almacenada del abonado que esté en posesión o bajo el control de dicho proveedor de servicios, cuando la información sobre el abonado sea necesaria para las investigaciones o procedimientos penales específicos de la Parte emisora.

2 a. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para que un proveedor de servicios en su territorio divulgue información sobre los abonados en respuesta a una orden en virtud del párrafo 1.

b. En el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, una Parte podrá – con respecto a las órdenes emitidas a los proveedores de servicios en su territorio – hacer la siguiente declaración: "La orden en virtud del párrafo 1 del artículo 7 debe ser emitida por un fiscal u otra autoridad judicial, o bajo su supervisión, o de lo contrario ser emitida bajo una supervisión independiente".

3. La orden a que se refiere el párrafo 1 deberá especificar:

a. la autoridad emisora y la fecha de emisión;

b. una declaración de que la orden se emite en virtud del presente Protocolo;

c. el nombre y la dirección del proveedor o proveedores de servicios que deben ser notificados;

d. el delito o delitos que son objeto de la investigación o el procedimiento penal;

e. la autoridad que solicita la información específica sobre el abonado, si no es la autoridad emisora, y

f. una descripción detallada de la información específica sobre el abonado que se busca.

4. La orden con arreglo al párrafo 1 irá acompañada de la siguiente información complementaria:

a. los fundamentos jurídicos internos que facultan a la autoridad para emitir la orden;

b. una referencia a las disposiciones legales y a las sanciones aplicables al delito objeto de investigación o enjuiciamiento;

c. la información de contacto de la autoridad a la que el proveedor de servicios deberá devolver la información del abonado, a la que podrá solicitar más información o a la que responderá de otro modo;

d. el periodo de tiempo para devolver la información del abonado y la forma de devolverla;

e. si ya se ha solicitado la conservación de los datos, incluida la fecha de conservación y cualquier número de referencia aplicable;

f. cualquier instrucción procesal especial;

g. si procede, una declaración de que se ha realizado una notificación simultánea de conformidad con el párrafo 5, y

h. cualquier otra información que pueda facilitar la obtención de la divulgación de la información del abonado.

5. a. Una Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, y en cualquier otro momento, notificar al Secretario General del Consejo de Europa que, cuando se emita una orden en virtud del párrafo 1 a un proveedor de servicios en su territorio, la Parte requiere, en todos los casos o en circunstancias determinadas, la notificación simultánea de la orden, la información complementaria y un resumen de los hechos relacionados con la investigación o el procedimiento.

b. Independientemente de que una Parte exija o no la notificación en virtud del párrafo 5.a, podrá exigir al proveedor de servicios que consulte a las autoridades de la Parte en circunstancias determinadas antes de la divulgación.

c. Las autoridades notificadas con arreglo al párrafo 5.a o consultadas con arreglo al párrafo 5.b podrán, sin demora injustificada, ordenar al proveedor de servicios que no divulgue la información sobre el abonado si:

i. la divulgación puede perjudicar las investigaciones o procedimientos penales en esa Parte, o

ii. las condiciones o los motivos de denegación se aplicarían en virtud del párrafo 4 del artículo 25 y del párrafo 4 del artículo 27 del Convenio si la información sobre el abonado se hubiera recabado mediante asistencia mutua.

d. Las autoridades notificadas en virtud del párrafo 5.a o consultadas en virtud del párrafo 5.b:

i. podrán solicitar información adicional a la autoridad mencionada en el párrafo 4.c a los efectos de la aplicación del párrafo 5.c y no la divulgarán al proveedor de servicios sin el consentimiento de dicha autoridad, y

ii. informarán sin demora a la autoridad mencionada en el párrafo 4.c si el proveedor de servicios ha recibido instrucciones de no divulgar la información sobre el abonado y expondrán los motivos para ello.

e. Una Parte designará una única autoridad para recibir la notificación de conformidad con el párrafo 5.a y para llevar a cabo las acciones descritas en los párrafos 5.b, 5.c y 5.d. La Parte, en el momento de la primera notificación al

Secretario General del Consejo de Europa de conformidad con el párrafo 5.a, deberá comunicar al Secretario General la información de contacto de dicha autoridad.

f. El Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de las autoridades designadas por las Partes de conformidad con el párrafo 5.e y de si requieren una notificación en virtud del párrafo 5.a y en qué circunstancias. Cada Parte se asegurará de que los datos que proporcione para el registro sean correctos en todo momento.

6. Si es aceptable para el proveedor de servicios, una Parte podrá presentar una orden en virtud del párrafo 1 y la información complementaria de conformidad con el párrafo 4 en formato electrónico. Una Parte podrá presentar la notificación y la información complementaria de conformidad con el párrafo 5 en forma electrónica. Es posible que se requieran niveles adecuados de seguridad y autentificación.

7. Si un proveedor de servicios informa a la autoridad en el párrafo 4.c que no divulgará la información sobre el abonado solicitada, o si no divulga la información sobre el abonado en respuesta a la orden en virtud del párrafo 1 en un plazo de treinta días a partir de la recepción de la orden o del plazo estipulado en el párrafo 4.d, si éste es más largo, las autoridades competentes de la Parte emisora podrán entonces solicitar la ejecución de la orden únicamente a través del artículo 8 u otras formas de asistencia mutua. Las Partes podrán solicitar a un proveedor de servicios que dé una razón para negarse a divulgar la información del abonado solicitada por la orden.

8. Una Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que la Parte emisora deberá solicitar al proveedor de servicios la divulgación de la información sobre los abonados antes de solicitarla en virtud del artículo 8, a menos que la Parte emisora dé una explicación razonable por no haberlo hecho.

9. En el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, una Parte podrá:

a. reservarse el derecho de no aplicar este artículo, o

b. si la divulgación de determinados tipos de números de acceso en virtud de este artículo fuera incompatible con los principios fundamentales

de su ordenamiento jurídico interno, reservarse el derecho de no aplicar este artículo a dichos números.

Sección 3 - Procedimientos para mejorar la cooperación internacional entre autoridades para la divulgación de datos informáticos almacenados

Artículo 8 - Dar efecto a las órdenes de otra Parte para la producción acelerada de información sobre los abonados y datos de tráfico

1. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para emitir una orden que se presentará como parte de una solicitud a otra Parte con el fin de obligar a un proveedor de servicios en el territorio de la Parte requerida a presentar [información] específica y almacenada

a. información sobre los abonados, y

b. datos de tráfico en posesión o control de dicho proveedor de servicios que sean necesarios para las investigaciones o procedimientos penales específicos de la Parte.

2. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para dar efecto a una orden en virtud del párrafo 1 presentada por una Parte requirente.

3. En su solicitud, la Parte requirente presentará a la Parte requerida la orden prevista en el párrafo 1, la información de apoyo y cualquier instrucción especial de procedimiento.

a La orden deberá especificar:

i. la autoridad emisora y la fecha de emisión de la orden;

ii. una declaración de que la orden se presenta en virtud del presente Protocolo;

iii. el nombre y la dirección del proveedor o proveedores de servicios que deben ser notificados;

iv. el delito o delitos que son objeto de la investigación o procedimiento penal;

v. la autoridad que solicita la información o los datos, si no es la autoridad emisora, y

vi. una descripción detallada de la información o los datos concretos solicitados.

b. La información de apoyo, proporcionada con el fin de ayudar a la Parte requerida a dar efecto a la orden y que no se divulgará al proveedor de servicios sin el consentimiento de la Parte requirente, especificará:

i. los fundamentos jurídicos internos que facultan a la autoridad para emitir la orden;

ii. las disposiciones legales y las sanciones aplicables al delito o delitos objeto de investigación o enjuiciamiento;

iii. el motivo por el que la Parte requirente cree que el proveedor de servicios está en posesión o control de los datos;

iv. un resumen de los hechos relacionados con la investigación o el procedimiento;

v. la pertinencia de la información o los datos para la investigación o el procedimiento;

vi. información de contacto de una autoridad o autoridades que puedan proporcionar más información;

vii. si ya se ha solicitado la conservación de la información o de los datos, incluida la fecha de conservación y cualquier número de referencia aplicable, y

viii. si la información o los datos ya se han recabado por otros medios y, en su caso, de qué manera.

c. La Parte requirente podrá solicitar que la Parte requerida lleve a cabo instrucciones procesales especiales.

4 Una Parte podrá declarar en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, y en cualquier otro momento, que se requiere información justificativa adicional para dar efecto a las órdenes del párrafo 1.

5 La Parte requerida aceptará las solicitudes en formato electrónico. Podrá exigir niveles adecuados de seguridad y autentificación antes de aceptar la solicitud.

6. a. La Parte requerida, a partir de la fecha de recepción de toda la información especificada en los párrafos 3 y 4, hará esfuerzos razonables para notificar al proveedor de servicios en un plazo de cuarenta y cinco días, si no antes, y ordenará la devolución de la información o los datos solicitados a más tardar:

i. veinte días para la información de los abonados, y

ii. cuarenta y cinco días para los datos de tráfico.

b. La Parte requerida dispondrá la transmisión de la información o los datos producidos a la Parte requirente sin demora indebida.

7. Si la Parte requerida no puede cumplir las instrucciones del párrafo 3.c en la forma solicitada, informará sin demora a la Parte requirente y, si procede, especificará las condiciones en las que podría cumplirlas, tras lo cual la Parte requirente determinará si, a pesar de todo, la solicitud debe ser ejecutada.

8. La Parte requerida podrá negarse a ejecutar una solicitud por los motivos establecidos en el párrafo 4 del artículo 25, o en el párrafo 4 del artículo 27 del Convenio, o podrá imponer las condiciones que considere necesarias para permitir la ejecución de la solicitud. La Parte requerida podrá aplazar la ejecución de las solicitudes por los motivos establecidos en el párrafo 5 del artículo 27 del Convenio. La Parte requerida notificará a la Parte requirente, tan pronto como sea posible, la denegación, las condiciones o el aplazamiento. La Parte requerida notificará también a la Parte requirente otras circunstancias que puedan retrasar significativamente la ejecución de la solicitud. El artículo 28, párrafo 2.b, del Convenio se aplicará al presente artículo.

9. a. Si la Parte requirente no puede cumplir una condición impuesta por la Parte requerida en virtud del párrafo 8, informará sin demora a la Parte requerida. La Parte requerida determinará entonces si, a pesar de ello, debe facilitarse la información o el material.

b. Si la Parte requirente acepta la condición, quedará obligada a cumplirla. La Parte requerida que suministre información o material sujeto a dicha condición podrá exigir a la Parte requirente que explique, en relación con dicha condición, el uso que se ha hecho de dicha información o material.

10. Cada Parte, en el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, comunicará al Secretario General del Consejo de Europa y mantendrá actualizada la información de contacto de las autoridades designadas:

a. para presentar una orden en virtud del presente artículo, y

b. para recibir una orden en virtud del presente artículo.

11. Una Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que exige que las solicitudes de otras Partes en virtud del presente artículo le sean presentadas por la autoridad central de la Parte requirente, o por cualquier otra autoridad que las Partes interesadas determinen de común acuerdo.

12. El Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de las autoridades designadas por las Partes en virtud del párrafo 10. Cada Parte se asegurará de que los datos que haya facilitado para el registro sean correctos en todo momento.

13. En el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, una Parte podrá reservarse el derecho de no aplicar el presente artículo a los datos de tráfico.

Artículo 9 - Divulgación acelerada de datos informáticos almacenados en caso de emergencia

1. a. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias, en caso de emergencia, para que su punto de contacto para la Red 24/7 a que se hace referencia en el artículo 35 del Convenio ("punto de contacto") pueda transmitir una solicitud a un punto de contacto de otra Parte y recibir una solicitud de éste en la que se pida asistencia inmediata para obtener de un proveedor de servicios en el territorio de esa Parte la divulgación acelerada de determinados datos informáticos almacenados que estén en posesión o bajo el control de ese proveedor de servicios, sin necesidad de una solicitud de asistencia mutua.

b. Una Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que no dará cumplimiento a las solicitudes contempladas en el párrafo 1.a que pretendan únicamente la divulgación de la información de los abonados.

2. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para permitir, de conformidad con el párrafo 1:

a. que sus autoridades puedan recabar datos de un proveedor de servicios en su territorio a raíz de una solicitud en virtud del párrafo 1;

b. que un proveedor de servicios en su territorio divulgue los datos solicitados a sus autoridades en respuesta a una solicitud en virtud del párrafo 2.a, y

c. que sus autoridades faciliten los datos solicitados a la Parte requirente.

3. La solicitud en virtud del párrafo 1 deberá especificar:

a. la autoridad competente que solicita los datos y la fecha en que se emitió la solicitud;

b. una declaración de que la solicitud se emite en virtud del presente Protocolo;

c. el nombre y la dirección del proveedor o proveedores de servicios en posesión o control de los datos solicitados;

d. el delito o delitos objeto de la investigación o procedimiento penal y una referencia a sus disposiciones jurídicas y a las penas aplicables;

e. hechos suficientes para demostrar que existe una emergencia y cómo los datos buscados se relacionan con ella;

f. una descripción detallada de los datos solicitados;

g. cualquier instrucción especial de procedimiento, y

h. cualquier otra información que pueda facilitar la obtención de la divulgación de los datos solicitados.

4. La Parte requerida aceptará una solicitud en formato electrónico. Una Parte también podrá aceptar una solicitud transmitida verbalmente y podrá exigir confirmación en forma electrónica. Podrá exigir niveles adecuados de seguridad y autentificación antes de aceptar la solicitud.

5. Una Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que exige a las Partes requirentes, tras la ejecución de la solicitud, que presenten la solicitud y cualquier información complementaria transmitida en apoyo de la misma, en el formato y por el conducto, que podrá incluir la asistencia mutua, que especifique la Parte requerida.

6. La Parte requerida informará a la Parte requirente de su decisión sobre la solicitud en virtud del párrafo 1 de forma rápida y expedita y, si procede, especificará las condiciones en las que proporcionaría los datos y cualquier otra forma de cooperación de que se disponga.

7. a. Si una Parte requirente no puede cumplir una condición impuesta por la Parte requerida en virtud del párrafo 6, informará sin demora a la Parte requerida. La Parte requerida determinará entonces si la información o el material deben proporcionarse de todos modos. Si la Parte requirente acepta la condición, quedará obligada a cumplirla.

b. La Parte requerida que suministre información o material sujeto a dicha condición podrá exigir a la Parte requirente que explique, en relación con dicha condición, el uso que se hace de dicha información o material.

Sección 4 – Procedimientos relativos a la asistencia mutua en caso de emergencia

Artículo 10 - Asistencia mutua en caso de emergencia

1. Cada Parte podrá solicitar asistencia mutua de forma rápida y expedita cuando considere que existe una emergencia. Una solicitud en virtud del presente artículo deberá incluir, además de los demás elementos necesarios, una descripción de los hechos que demuestran que existe una emergencia y la forma en que la asistencia solicitada se relaciona con ella.

2. La Parte requerida aceptará dicha solicitud en formato electrónico. Podrá exigir niveles adecuados de seguridad y autentificación antes de aceptar la solicitud.

3. La Parte requerida podrá solicitar, de forma rápida y expedita, información complementaria para evaluar la solicitud. La Parte requirente facilitará dicha información complementaria de forma rápida y expedita.

4. Una vez que esté convencida de que existe una emergencia y de que se han cumplido los demás requisitos de asistencia mutua, la Parte requerida responderá a la solicitud de forma rápida y expedita.

5. Cada Parte garantizará que una persona de su autoridad central o de otras autoridades responsables de responder a las solicitudes de asistencia mutua esté disponible las veinticuatro horas del día y los siete días de la semana para responder a una solicitud de conformidad con el presente artículo.

6. La autoridad central u otras autoridades responsables de la asistencia mutua de la Parte requirente y de la Parte requerida podrán determinar de común acuerdo que los resultados de la ejecución de una solicitud en virtud del presente artículo, o una copia anticipada de los mismos, puedan facilitarse a la Parte requirente por un cauce distinto del utilizado para la solicitud.

7. Cuando no exista un tratado o acuerdo de asistencia mutua basado en una legislación uniforme o recíproca en vigor entre las Partes requirente y requerida, se aplicarán al presente artículo los párrafos 2.b y 3 a 8 del artículo 27, y los párrafos 2 a 4 del artículo 28 del Convenio.

8. Cuando exista tal tratado o acuerdo, el presente artículo se complementará con las disposiciones de dicho tratado o acuerdo, a menos que las Partes interesadas decidan de común acuerdo aplicar, en su lugar, alguna o todas las disposiciones del Convenio a que se hace referencia en el párrafo 7 del presente artículo.

9. Cada Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que las solicitudes también podrán ser enviadas directamente a sus autoridades judiciales, o a través de los canales de la Organización Internacional de Policía Criminal (INTERPOL) o a su punto de contacto 24/7 establecido en virtud del artículo 35 del Convenio. En cualquiera de estos casos, se enviará al mismo tiempo una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente. Cuando una solicitud se envíe directamente a una autoridad judicial de la Parte requerida y ésta no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará a la Parte requirente directamente de que lo ha hecho.

Sección 5 - Procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables

Artículo 11 - Videoconferencia

1. Una Parte requirente podrá solicitar, y la Parte requerida podrá permitir, que se tomen testimonios y declaraciones de un testigo o perito por videoconferencia. La Parte requirente y la Parte requerida se consultarán para facilitar la resolución de cualquier cuestión que pueda surgir en relación con la ejecución de la solicitud, incluyendo, según proceda: qué Parte presidirá; las autoridades y personas que estarán presentes; si una o ambas Partes administrarán juramentos y advertencias o proporcionarán instrucciones particulares al testigo o perito; la manera de interrogar al testigo o perito; la manera en que se garantizarán debidamente los derechos del testigo o perito; el tratamiento de las reclamaciones de privilegio o inmunidad; el tratamiento de las objeciones a las preguntas o respuestas, y si una o ambas Partes proporcionarán servicios de traducción, interpretación y transcripción.

2. a. Las autoridades centrales de las Partes requerida y requirente se comunicarán directamente entre sí a efectos del presente artículo. La Parte requerida podrá aceptar una solicitud en formato electrónico. Podrá exigir niveles adecuados de seguridad y autentificación antes de aceptar la solicitud.

b. La Parte requerida informará a la Parte requirente de los motivos por los que no ejecuta o retrasa la ejecución de la solicitud. El párrafo 8 del artículo 27 del Convenio se aplica al presente artículo. Sin perjuicio de cualquier otra condición que una Parte requerida pueda imponer de conformidad con el presente artículo, se aplican al presente artículo los párrafos 2 a 4 del artículo 28 del Convenio.

3. La Parte requerida que preste asistencia en virtud del presente artículo procurará obtener la presencia de la persona cuyo testimonio o declaración se solicita. Cuando proceda, la Parte requerida podrá, en la medida en que lo permita su legislación, adoptar las medidas necesarias para obligar a un testigo o perito a comparecer en la Parte requerida en un momento y lugar determinados.

4. Se seguirán los procedimientos relativos a la realización de la videoconferencia especificados por la Parte requirente, salvo que sean incompatibles con la legislación nacional de la Parte requerida. En caso de incompatibilidad, o en la medida en que el procedimiento no haya sido especificado por la Parte requirente, la Parte requerida aplicará el procedimiento previsto en su legislación nacional, salvo que las Partes requirente y requerida decidan de común acuerdo otra cosa.

5. Sin perjuicio de la competencia con arreglo al derecho interno de la Parte requirente, cuando en el transcurso de la videoconferencia, el testigo o perito:

a. haga una declaración intencionadamente falsa cuando la Parte requerida, de conformidad con la legislación nacional de la Parte requerida, haya obligado a dicha persona a testificar con veracidad;

b. se niegue a testificar cuando la Parte requerida, de conformidad con su derecho interno, haya obligado a dicha persona a testificar, o

c. cometa otra falta prohibida por el derecho interno de la Parte requerida en el curso de dicho procedimiento, la persona será sancionable en la Parte requerida de la misma manera que si dicho acto se hubiera cometido en el curso de sus procedimientos internos.

6. a. Salvo que la Parte requirente y la Parte requerida determinen de común acuerdo otra cosa, la Parte requerida correrá con todos los gastos relacionados con la ejecución de una solicitud en virtud del presente artículo, excepto:

i. los honorarios de un perito;

ii. los gastos de traducción, interpretación y transcripción, y

iii. los gastos de carácter extraordinario.

b. Si la ejecución de una solicitud impusiera gastos de carácter extraordinario, la Parte requirente y la Parte requerida se consultarán mutuamente a fin de determinar las condiciones en las que puede ejecutarse la solicitud.

7. Cuando la Parte requirente y la Parte requerida lo hayan acordado mutuamente:

a. las disposiciones del presente artículo podrán aplicarse a efectos de la realización de audioconferencias, y

b. la tecnología de videoconferencia podrá utilizarse para fines, o para audiencias, distintos de los descritos en el párrafo 1, incluso para fines de identificación de personas u objetos.

8. Cuando una Parte requerida opte por permitir la audiencia de un sospechoso o acusado, podrá exigir condiciones y salvaguardias particulares con respecto a la toma de testimonio o declaración de dicha persona, o a la entrega de notificaciones o la aplicación de medidas procesales a la misma.

Artículo 12 - Equipos conjuntos de investigación e investigaciones conjuntas

1. Por acuerdo mutuo, las autoridades competentes de dos o más Partes podrán establecer y poner en funcionamiento un equipo conjunto de investigación en sus territorios para facilitar las investigaciones o los procedimientos penales, cuando se considere de particular utilidad una mayor coordinación. Las autoridades competentes serán determinadas por las respectivas Partes interesadas.

2. Los procedimientos y condiciones que rijan el funcionamiento de los equipos conjuntos de investigación, tales como sus fines específicos; su composición; sus funciones; su duración y cualquier periodo de prórroga; su ubicación; su organización; las condiciones de recopilación, transmisión y utilización de la información o de las pruebas; las condiciones de confidencialidad, y las condiciones de participación de las autoridades de una Parte en las actividades de investigación que tengan lugar en el territorio de otra Parte, serán los acordados entre dichas autoridades competentes.

3. Una Parte podrá declarar, en el momento de la firma de este Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, que su autoridad central debe ser signataria del acuerdo por el que se establece el equipo o estar de otra manera de acuerdo con él.

4. Dichas autoridades competentes y participantes se comunicarán directamente, con la salvedad de que las Partes podrán determinar de común acuerdo otros canales de comunicación apropiados cuando circunstancias excepcionales requieran una coordinación más centralizada.

5. Cuando sea necesario adoptar medidas de investigación en el territorio de una de las Partes afectadas, las autoridades participantes de esa Parte

podrán solicitar a sus propias autoridades que adopten dichas medidas sin que las demás Partes tengan que presentar una solicitud de asistencia mutua. Dichas medidas serán llevadas a cabo por las autoridades de esa Parte en su territorio en las condiciones que se apliquen de conformidad con el derecho interno en una investigación nacional.

6. La utilización de la información o las pruebas facilitadas por las autoridades participantes de una Parte a las autoridades participantes de otras Partes afectadas podrá denegarse o restringirse de la manera establecida en el acuerdo descrito en los párrafos 1 y 2. Si dicho acuerdo no establece las condiciones para denegar o restringir el uso, las Partes podrán utilizar la información o los elementos de prueba facilitados:

a. para los fines para los que se ha celebrado el acuerdo;

b. para la detección, investigación y persecución de delitos distintos de aquellos para los que se celebró el acuerdo, previo consentimiento de las autoridades que proporcionaron la información o las pruebas. No obstante, no se requerirá el consentimiento cuando los principios jurídicos fundamentales de la Parte que utilice la información o las pruebas exijan que divulgue la información o las pruebas para proteger los derechos de una persona acusada en un proceso penal. En tal caso, dichas autoridades notificarán sin demora injustificada a las autoridades que proporcionaron la información o las pruebas, o

c. para prevenir una emergencia. En tal caso, las autoridades participantes que hayan recibido la información o las pruebas lo notificarán sin demora injustificada a las autoridades participantes que hayan proporcionado la información o las pruebas, a menos que se determine lo contrario de mutuo acuerdo.

7. A falta de un acuerdo como los descritos en los párrafos 1 y 2, se podrán realizar investigaciones conjuntas en condiciones convenidas mutuamente caso por caso. El presente párrafo se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua basado en una legislación uniforme o recíproca en vigor entre las Partes interesadas.

Capítulo III - Condiciones y salvaguardias

Artículo 13 - Condiciones y salvaguardias

De conformidad con el artículo 15 del Convenio, cada Parte velará por que el establecimiento, la ejecución y la aplicación de las facultades y los procedimientos previstos en el presente Protocolo estén sujetos a las condiciones

y salvaguardias previstas en su derecho interno, que deberá garantizar la protección adecuada de los derechos humanos y las libertades.

Artículo 14 - Protección de datos personales

1. Ámbito de aplicación

a. Salvo que se disponga lo contrario en los párrafos 1.b y c, cada Parte procesará los datos personales que reciba en virtud del presente Protocolo de conformidad con los párrafos 2 a 15 del presente artículo.

b. Si, en el momento de la recepción de los datos personales en virtud del presente Protocolo, tanto la Parte transferente como la Parte receptora están mutuamente vinculadas por un acuerdo internacional que establezca un marco global entre dichas Partes para la protección de datos personales que sea aplicable a la transferencia de datos personales con fines de prevención, detección, investigación y enjuiciamiento de delitos penales, y que disponga que el tratamiento de datos personales en virtud de dicho acuerdo cumple con los requisitos de la legislación sobre protección de datos de las Partes afectadas, los términos de dicho acuerdo se aplicarán, para las medidas que entren en su ámbito de aplicación, a los datos personales recibidos en virtud del Protocolo en lugar de los párrafos 2 a 15, a menos que las Partes interesadas acuerden otra cosa.

c. Si la Parte transferente y la Parte receptora no están mutuamente vinculadas en virtud de un acuerdo descrito en el párrafo 1.b, podrán determinar mutuamente que la transferencia de datos personales en virtud del presente Protocolo pueda tener lugar sobre la base de otros acuerdos o arreglos entre las Partes interesadas en lugar de los párrafos 2 a 15.

d. Cada Parte considerará que el tratamiento de datos personales con arreglo a los párrafos 1.a y 1.b cumple los requisitos de su marco jurídico de protección de datos personales para las transferencias internacionales de datos personales, y no se requerirá ninguna otra autorización para la transferencia con arreglo a dicho marco jurídico. Una Parte sólo podrá denegar o impedir las transferencias de datos a otra Parte en virtud del presente Protocolo por motivos de protección de datos en las condiciones establecidas en el párrafo 15 cuando se aplique el párrafo 1.a, o en virtud de los términos de un acuerdo o convenio a que se hace referencia en los párrafos 1.b o c, cuando sea aplicable uno de esos párrafos.

e. Nada de lo dispuesto en el presente artículo impedirá que una Parte aplique salvaguardias más estrictas al tratamiento por sus propias autoridades de los datos personales recibidos en virtud del presente Protocolo.

2. Finalidad y uso

a. La Parte que ha recibido datos personales procederá a su tratamiento para los fines descritos en el artículo 2. No hará tratamiento adicional de los datos personales con una finalidad incompatible y no someterá los datos a tratamiento ulterior cuando no lo permita su marco jurídico nacional. El presente artículo no afectará la capacidad de la Parte transferente de imponer condiciones adicionales en virtud del presente Protocolo en un caso concreto; no obstante, esas condiciones no incluirán condiciones genéricas de protección de datos.

b. La Parte receptora garantizará, con arreglo a su marco jurídico interno, que los datos personales solicitados y tratados sean pertinentes y no excesivos en relación con los fines de dicho tratamiento.

3. Calidad e integridad

Cada Parte adoptará medidas razonables para garantizar que los datos personales se mantengan con la exactitud e integridad y estén tan actualizados como sea necesario y adecuado para el tratamiento legítimo de los datos personales, teniendo en cuenta los fines del tratamiento de los mismos.

4. Datos sensibles

El tratamiento por una Parte de datos personales que revelen el origen racial o étnico; las opiniones políticas; las creencias religiosas o de otro tipo; la afiliación sindical; los datos genéticos; los datos biométricos considerados sensibles en vista de los riesgos que entrañan, o los datos personales relativos a la salud o a la vida sexual, sólo se llevará a cabo con las garantías adecuadas para evitar el riesgo de efectos perjudiciales injustificados del uso de dichos datos, en particular contra la discriminación ilegal.

5. Periodos de conservación

Cada una de las Partes conservará los datos personales solo durante el tiempo que sea necesario y procedente para los fines del tratamiento de los datos de conformidad con el párrafo 2. Con el fin de cumplir esta obligación, establecerá en su marco jurídico interno periodos de conservación específicos o revisiones periódicas de la necesidad de seguir conservando los datos.

6. Decisiones automatizadas

Las decisiones que produzcan un efecto negativo significativo en relación con los intereses pertinentes de la persona a la que se refieran los datos personales no podrán basarse únicamente en el tratamiento automatizado de datos

personales, a menos que lo autorice la legislación nacional y existan las garantías adecuadas que incluyan la posibilidad de obtener la intervención humana.

7. Seguridad de los datos e incidentes de seguridad

a. Cada Parte garantizará que dispone de las medidas tecnológicas, físicas y organizativas adecuadas para la protección de los datos personales, en particular contra la pérdida o el acceso accidental o no autorizado, la divulgación, la alteración o la destrucción ("incidente de seguridad").

b. Cuando se descubra un incidente de seguridad en el que exista un riesgo significativo de daño físico o no físico para las personas o para la otra Parte, la Parte receptora evaluará sin demora la probabilidad y la magnitud del mismo, y adoptará sin demora las medidas apropiadas para mitigar ese daño. Dichas medidas incluirán la notificación a la autoridad transferente o, a efectos de la sección 2 del capítulo II, a la autoridad o las autoridades designadas de conformidad con el párrafo 7. No obstante, la notificación podrá incluir restricciones adecuadas en cuanto a la transmisión ulterior de la notificación; podrá retrasarse u omitirse cuando dicha notificación pueda poner en peligro la seguridad nacional, o retrasarse cuando dicha notificación pueda poner en peligro las medidas de protección de la seguridad pública. Dichas medidas incluirán también la notificación a la persona afectada, a menos que la Parte haya tomado las medidas adecuadas para que ya no exista un riesgo significativo. La notificación a la persona podrá retrasarse u omitirse en las condiciones establecidas en el párrafo 12.a.i. La Parte notificada podrá solicitar consultas e información adicional sobre el incidente y la respuesta al mismo.

c. Cada Parte, en el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, comunicará al Secretario General del Consejo de Europa la autoridad o autoridades que han de ser notificadas de conformidad con el párrafo 7 a efectos de la sección 2 del capítulo II; la información proporcionada podrá modificarse posteriormente.

8. Mantenimiento de registros

Cada Parte mantendrá registros o dispondrá de otros medios apropiados para demostrar cómo se accede, utiliza y divulga los datos personales de una persona en un caso concreto.

9. Intercambio de información dentro de una Parte

a. Cuando una autoridad de una Parte proporcione datos personales recibidos inicialmente en virtud del presente Protocolo a otra autoridad de esa

Parte, esa otra autoridad procederá a su tratamiento de conformidad con el presente artículo, sin perjuicio de lo dispuesto en el párrafo 9.b.

b. No obstante lo dispuesto en el párrafo 9.a, una Parte que haya formulado una reserva en virtud del artículo 17 podrá facilitar los datos personales que haya recibido a sus Estados constituyentes o a entidades territoriales similares, siempre que la Parte haya adoptado medidas para que las autoridades receptoras sigan protegiendo eficazmente los datos, al proporcionar un nivel de protección de los mismos comparable al que ofrece el presente artículo.

c. En caso de que existan indicios de aplicación indebida del presente párrafo, la Parte transferente podrá solicitar consultas y la información pertinente sobre dichos indicios.

10. Transferencia ulterior a otro Estado u organización internacional

a. La Parte receptora podrá transferir los datos personales a otro Estado u organización internacional únicamente con la autorización previa de la autoridad transferente o, a efectos de la sección 2 del capítulo II, de la autoridad o autoridades designadas de conformidad con el párrafo 10.b.

b. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, la autoridad o autoridades que concederán autorización a efectos de la sección 2 del capítulo II; la información proporcionada podrá modificarse posteriormente.

11. Transparencia y notificación

a. Cada Parte notificará mediante la publicación de avisos generales, o mediante notificación personal a la persona cuyos datos personales se hayan recopilado, con respecto a:

i. la base jurídica y la finalidad del tratamiento;

ii. los periodos de conservación o revisión de conformidad con el párrafo 5, según corresponda;

iii. los destinatarios o categorías de destinatarios a los que se divulgan dichos datos, y

iv. el acceso, la rectificación y la reparación disponibles.

b. Una Parte podrá someter cualquier requisito de notificación personal a restricciones razonables con arreglo a su marco jurídico nacional de conformidad con las condiciones establecidas en el párrafo 12.a.i.

c. Cuando el marco jurídico nacional de la Parte transferente exija dar aviso personal a la persona cuyos datos han sido proporcionados a otra Parte, la Parte transferente adoptará medidas para que la otra Parte sea informada en el momento de la transferencia con respecto a este requisito y reciba la información de contacto adecuada. La notificación personal no se realizará si la otra Parte ha solicitado que la provisión de los datos se mantenga confidencial, cuando se apliquen las condiciones de restricción establecidas en el párrafo 12.a.i. Una vez que dejen de aplicarse estas restricciones y se pueda proporcionar la notificación personal, la otra Parte tomará medidas para que se informe a la Parte transferente. Si aún no ha sido informada, la Parte transferente tiene derecho a presentar solicitudes a la Parte receptora, la que informará a la Parte transferente si mantiene la restricción.

12. Acceso y rectificación

a. Cada Parte velará por que toda persona cuyos datos personales se hayan recibido en virtud del presente Protocolo tenga derecho a solicitar y obtener, de conformidad con los procedimientos establecidos en su ordenamiento jurídico interno y sin demora injustificada:

i. una copia escrita o electrónica de la documentación conservada sobre esa persona que contenga sus datos personales y la información disponible que indique la base jurídica y los fines del tratamiento, los periodos de conservación y los destinatarios o las categorías de destinatarios de los datos ("acceso"), así como información relativa a las opciones disponibles para obtener reparación; siempre que el acceso en un caso concreto pueda estar sujeto a la aplicación de restricciones proporcionadas permitidas en virtud de su marco jurídico interno, necesarias, en el momento del fallo, para proteger los derechos y las libertades de otras personas u objetivos importantes de interés público general y que tengan debidamente en cuenta los intereses legítimos de la persona afectada, y

ii. rectificación cuando los datos personales de la persona sean inexactos o hayan sido tratados incorrectamente; la rectificación incluirá – según corresponda y sea razonable teniendo en cuenta los motivos de la rectificación y el contexto particular del tratamiento – la corrección, la complementación, la supresión o la anonimización, la restricción del tratamiento o el bloqueo.

b. Si se deniega o restringe el acceso o la rectificación, la Parte proporcionará a la persona, por escrito, que podrá ser por vía electrónica, sin demora

injustificada, una respuesta en la que se le informe de la denegación o la restricción. En ella se expondrán los motivos de dicha denegación o restricción y se proporcionará información sobre las opciones de recurso disponibles. Cualquier gasto incurrido para obtener acceso deberá limitarse a lo que sea razonable y no excesivo.

13. Recursos judiciales y extrajudiciales

Cada Parte dispondrá de recursos judiciales y no judiciales efectivos para ofrecer reparación por las violaciones del presente artículo.

14. Supervisión

Cada Parte dispondrá de una o varias autoridades públicas que ejerzan, por sí solas o de forma acumulativa, funciones y facultades de supervisión independientes y eficaces con respecto a las medidas establecidas en el presente artículo. Entre las funciones y facultades de estas autoridades, actuando por si solas o acumulativamente, figurarán las facultades de investigación, la facultad para actuar en función de las denuncias y la capacidad de adoptar medidas correctivas.

15. Consulta y suspensión

Una Parte podrá suspender la transferencia de datos personales a otra Parte si tiene pruebas sustanciales de que la otra Parte incumple sistemática o materialmente los términos del presente artículo o de que es inminente un incumplimiento material. No suspenderá las transferencias sin previo aviso razonable, y no lo hará hasta después de que las Partes afectadas hayan iniciado un periodo razonable de consultas sin llegar a una resolución. No obstante, una Parte podrá suspender provisionalmente las transferencias en caso de una infracción sistemática o material que suponga un riesgo significativo e inminente para la vida o la seguridad de una persona física, o un daño sustancial a su reputación o su situación económica, en cuyo caso lo notificará a la otra Parte e iniciará consultas con ella inmediatamente después. Si las consultas no han conducido a una resolución, la otra Parte podrá suspender recíprocamente las transferencias si tiene pruebas sustanciales de que la suspensión por parte de la Parte que suspende era contraria a los términos de este párrafo. La Parte que suspende levantará la suspensión tan pronto como se haya subsanado la infracción que justifica la suspensión; cualquier suspensión recíproca se levantará en ese momento. Los datos personales transferidos antes de la suspensión seguirán siendo tratados de conformidad con el presente Protocolo.

Capítulo IV - Disposiciones finales

Artículo 15 - Efectos del presente Protocolo

1. a. El párrafo 2 del artículo 39 del Convenio se aplicará al presente Protocolo.

b. Con respecto a las Partes que son miembros de la Unión Europea, dichas Partes podrán, en sus relaciones mutuas, aplicar la legislación de la Unión Europea que rija las cuestiones tratadas en el presente Protocolo.

c. El párrafo 1.b no afecta a la plena aplicación del presente Protocolo entre las Partes que son miembros de la Unión Europea y las demás Partes.

2. El párrafo 3 del artículo 39 del Convenio se aplicará al presente Protocolo.

Artículo 16 - Firma y entrada en vigor

1. El presente Protocolo estará abierto a la firma de las Partes en el Convenio, que podrán expresar su consentimiento en obligarse mediante:

a. la firma sin reservas en cuanto a ratificación, aceptación o aprobación, o

b. la firma sujeta a ratificación, aceptación o aprobación, seguida de ratificación, aceptación o aprobación.

2. Los instrumentos de ratificación, aceptación o aprobación se depositarán ante el Secretario General del Consejo de Europa.

3. El presente Protocolo entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses a partir de la fecha en que cinco Partes en el Convenio hayan expresado su consentimiento en obligarse por el presente Protocolo, de conformidad con lo dispuesto en los párrafos 1 y 2 del presente artículo.

4. Respecto de toda Parte en el Convenio que manifieste posteriormente su consentimiento en quedar obligada por el presente Protocolo, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses a partir de la fecha en que la Parte haya expresado su consentimiento en quedar obligada por el presente Protocolo, de conformidad con lo dispuesto en los párrafos 1 y 2 del presente artículo.

Artículo 17 - Cláusula federal

1. Un Estado federal podrá reservarse el derecho de asumir obligaciones en virtud del presente Protocolo, que sean compatibles con los principios

fundamentales que rigen las relaciones entre su gobierno central y los Estados constituyentes u otras entidades territoriales similares, siempre que:

a. el Protocolo se aplique al gobierno central del Estado federal;

b. dicha reserva no afecte a las obligaciones de proporcionar la cooperación solicitada por otras Partes de conformidad con las disposiciones del capítulo II, y

c. las disposiciones del artículo 13 se apliquen a los Estados constituyentes del Estado federal o a otras entidades territoriales similares.

2. Otra Parte podrá impedir que las autoridades, proveedores o entidades en su territorio cooperen en respuesta a una solicitud u orden presentada directamente por el Estado constituyente u otra entidad territorial similar de un Estado federal que haya formulado una reserva en virtud del párrafo 1, a menos que dicho Estado federal notifique al Secretario General del Consejo de Europa que un Estado constituyente u otra entidad territorial similar aplica las obligaciones del presente Protocolo aplicables a dicho Estado federal. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de dichas notificaciones.

3. Otra Parte no impedirá que las autoridades, los proveedores o las entidades de su territorio cooperen con un Estado constituyente u otra entidad territorial similar en virtud de una reserva formulada con arreglo al párrafo 1, si se ha presentado una orden o una solicitud a través del gobierno central o se ha celebrado un acuerdo de equipo conjunto de investigación con arreglo al artículo 12 con la participación del Gobierno central. En tales situaciones, el gobierno central velará por el cumplimiento de las obligaciones aplicables del Protocolo, siempre que, con respecto a la protección de los datos personales facilitados a los Estados constituyentes o entidades territoriales similares, solamente se aplicarán los términos del párrafo 9 del artículo 14 o, cuando proceda, las disposiciones de un acuerdo o convenio descrito en los párrafos 1.b o 1.c del artículo 14.

4. En lo que respecta a las disposiciones del presente Protocolo cuya aplicación sea competencia de los Estados constituyentes o de otras entidades territoriales similares que no estén obligadas por el régimen constitucional de la federación a adoptar medidas legislativas, el gobierno central informará a las autoridades competentes de dichos Estados de dichas disposiciones con su dictamen favorable, instándoles a adoptar las medidas adecuadas para ponerlas en práctica.

Artículo 18 - Aplicación territorial

1. El presente Protocolo se aplicará al territorio o territorios especificados en una declaración hecha por una Parte en virtud de los párrafos 1 o 2 del artículo 38 del Convenio, en la medida en que dicha declaración no haya sido retirada con arreglo al párrafo 3 del artículo 38.

2. Una Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que el presente Protocolo no se aplicará a uno o más territorios especificados en la declaración de la Parte en virtud de los párrafos 1 y/o 2 del artículo 38 del Convenio.

3. Toda declaración hecha en virtud del párrafo 2 del presente artículo podrá retirarse, respecto de cualquier territorio especificado en dicha declaración, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses contado a partir de la fecha de recepción de dicha notificación por el Secretario General.

Artículo 19 - Reservas y declaraciones

1. Mediante notificación escrita dirigida al Secretario General del Consejo de Europa, toda Parte en el Convenio podrá, en el momento de la firma o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que se acoge a la reserva o reservas previstas en el artículo 7, párrafos 9.a y 9.b; en el artículo 8, párrafo 13, y en el artículo 17 del presente Protocolo. No podrán formularse otras reservas.

2. Mediante notificación escrita dirigida al Secretario General del Consejo de Europa, toda Parte en el Convenio podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, hacer la declaración o declaraciones indicadas en el artículo 7, párrafos 2.b y 8; en el artículo 8, párrafo 11; en el artículo 9, párrafos 1.b y 5; en el artículo 10, párrafo 9; en el artículo 12, párrafo 3, y en el artículo 18, párrafo 2, del presente Protocolo.

3. Mediante notificación escrita dirigida al Secretario General del Consejo de Europa, toda Parte en el Convenio hará cualquier declaración o notificaciones o comunicaciones mencionadas en el artículo 7, párrafos 5.a y e; en el artículo 8, párrafos 4 y 10.a y b; en el artículo 14, párrafos 7.c y 10.b, y en el artículo 17, párrafo 2, del presente Protocolo, con arreglo a los términos que se especifican en ellos.

Artículo 20 - Situación y retirada de las reservas

1. Una Parte que haya formulado una reserva de conformidad con el párrafo 1 del artículo 19 la retirará, total o parcialmente, tan pronto como las circunstancias lo permitan. Dicha retirada surtirá efecto en la fecha de recepción de una notificación dirigida al Secretario General del Consejo de Europa. Si en la notificación se indica que la retirada de una reserva surtirá efecto en la fecha especificada en ella, y esa fecha es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en esa fecha posterior.

2. El Secretario General del Consejo de Europa podrá consultar periódicamente a las Partes que hayan formulado una o varias reservas de conformidad con el párrafo 1 del artículo 19, sobre las perspectivas de retirarlas.

Artículo 21 - Enmiendas

1. Las enmiendas al presente Protocolo podrán ser propuestas por cualquiera de las Partes en el mismo y serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa y a las Partes y signatarios del Convenio, así como a cualquier Estado que haya sido invitado a adherirse al Convenio.

2. Toda enmienda propuesta por una Parte se comunicará al Comité Director para los Problemas Criminales (CDPC), que presentará al Comité de Ministros su dictamen sobre dicha propuesta de enmienda.

3. El Comité de Ministros examinará la propuesta de enmienda y el dictamen presentado por el CDPC y, previa consulta con las Partes en el Convenio, podrá adoptar la enmienda.

4. El texto de toda enmienda adoptada por el Comité de Ministros de conformidad con el párrafo 3 se remitirá a las Partes en el presente Protocolo para su aceptación.

5. Toda enmienda adoptada de conformidad con el párrafo 3 entrará en vigor el trigésimo día después de que todas las Partes en el presente Protocolo hayan informado al Secretario General de su aceptación.

Artículo 22 - Solución de controversias

El artículo 45 del Convenio se aplicará al presente Protocolo.

Artículo 23 - Consultas de las Partes y evaluación de la aplicación

1. El artículo 46 del Convenio se aplicará al presente Protocolo.

2. Las Partes evaluarán periódicamente la utilización y aplicación efectivas de las disposiciones del presente Protocolo. El artículo 2 del Reglamento Interno del Comité del Convenio sobre la Ciberdelincuencia, revisado el 16 de octubre de 2020, se aplicará *mutatis mutandis*. Las Partes revisarán inicialmente y podrán modificar por consenso los procedimientos de dicho artículo en la medida en que se apliquen al presente Protocolo cinco años después de la entrada en vigor del mismo.

3. La revisión del artículo 14 se iniciará una vez que diez Partes en el Convenio hayan expresado su consentimiento en obligarse por el presente Protocolo.

Artículo 24 - Denuncia

1. Cualquiera de las Partes podrá, en todo momento, denunciar el presente Protocolo mediante una notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses a partir de la fecha de recepción de la notificación por el Secretario General.

3. La denuncia del Convenio por una Parte en el presente Protocolo constituye una denuncia del presente Protocolo.

4. La información o las pruebas transferidas antes de la fecha efectiva de la denuncia seguirán siendo tratadas de conformidad con el presente Protocolo.

Artículo 25 - Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a las Partes y a los signatarios del Convenio, así como a todo Estado que haya sido invitado a adherirse al Convenio acerca de:

a. cualquier firma;

b. el depósito de cualquier instrumento de ratificación, aceptación o aprobación;

c. cualquier fecha de entrada en vigor del presente Protocolo de conformidad con los párrafos 3 y 4 del artículo 16;

d. toda declaración o reserva formulada de conformidad con el artículo 19 o la retirada de reservas formulada de conformidad con el artículo 20, y

e. cualquier otro acto, notificación o comunicación relacionados con el presente Protocolo.

Informe explicativo al Segundo Protocolo adicional

1. El Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas ("el presente Protocolo") fue adoptado por el Comité de Ministros del Consejo de Europa en la reunión 1417bis del 17 de noviembre de 2021 de los Delegados de los Ministros, y el presente Protocolo quedará abierto a la firma en Estrasburgo el 12 de mayo de 2022. El Comité de Ministros también tomó nota del informe explicativo.

2. El texto del presente informe explicativo tiene por objeto orientar y ayudar a las Partes en la aplicación del presente Protocolo y refleja la interpretación de quienes participaron en la redacción en cuanto a su funcionamiento.

Introducción

Antecedentes

3. El Convenio sobre la Ciberdelincuencia (STE nº 185; en adelante "el Convenio"), desde que fue abierto a la firma en Budapest el 23 de noviembre de 2001, se ha convertido en un instrumento que cuenta con miembros de todas las regiones del mundo y tiene un impacto mundial.

4. En 2003, el Convenio fue complementado por el Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE nº 189; en adelante, el "Primer Protocolo").

5. Desde que el Convenio se abrió a la firma en 2001, las tecnologías de la información y la comunicación han evolucionado y transformado las sociedades en todo el mundo de manera extraordinaria. Sin embargo, desde aquella fecha también se ha producido un aumento significativo de la explotación de esas tecnologías con fines delictivos. En la actualidad, muchas Partes consideran que la ciberdelincuencia constituye una grave amenaza para los derechos humanos, el estado de derecho y el funcionamiento de las sociedades democráticas. Las amenazas que plantea la ciberdelincuencia son numerosas. Algunos ejemplos son: la violencia sexual en línea contra los niños y otros delitos contra la dignidad y la integridad de las personas; el robo y la utilización indebida de los datos personales que afectan a la vida privada de las personas; la interferencia en los procesos electorales y otros ataques contra las instituciones democráticas; los ataques contra infraestructuras vitales, como la denegación de servicio distribuida y los ataques

de *ransomware*; o la utilización inapropiada de esas tecnologías con fines terroristas. En 2020 y 2021, durante la pandemia de covid-19, en diversos países se registraron numerosos casos de ciberdelincuencia relacionados con el virus, incluidos los ataques a hospitales e instalaciones médicas que desarrollan vacunas contra el virus; la utilización indebida de nombres de dominio para promover vacunas, tratamientos y curas falsas, y otros tipos de actividades fraudulentas.

6. A pesar del desarrollo de las tecnologías basadas en datos y de la perniciosa expansión y evolución de la ciberdelincuencia, los conceptos consagrados en el Convenio son neutrales desde el punto de vista tecnológico, de modo que el derecho penal sustantivo puede aplicarse tanto a las tecnologías actuales como a las futuras, y el Convenio sigue cumpliendo una función esencial en la lucha contra la ciberdelincuencia. El Convenio está orientado principalmente a: i) armonizar los elementos de derecho penal sustantivo interno de los delitos y las disposiciones conexas en materia de ciberdelincuencia; ii) establecer las facultades del derecho procesal penal interno necesarias para la investigación y el procesamiento de esos delitos, así como de otros delitos cometidos por medio de un sistema informático o relativos a la utilización de pruebas electrónicas de otros delitos, y iii) establecer un régimen rápido y eficiente de cooperación internacional.

7. En la aplicación del Convenio, las Partes respetan la responsabilidad que tienen los gobiernos de proteger a las personas contra la delincuencia, tanto si se comete en línea como en otros ámbitos, mediante investigaciones y enjuiciamientos penales eficaces. De hecho, algunas Partes en el Convenio consideran que tienen la obligación internacional de proporcionar los medios para la protección contra los delitos cometidos mediante un sistema informático (véase *K.U. c. Finlandia*, Tribunal Europeo de Derechos Humanos (Solicitud nº 2872/02; sentencia/decisión del 2 de marzo de 2009), en que se hace referencia a los procedimientos y facultades para las investigaciones o procesos penales que las Partes deben establecer en virtud del Convenio.

8. Las Partes han procurado incesantemente cumplir su compromiso en materia de lucha contra la ciberdelincuencia recurriendo a diversos mecanismos y órganos creados en virtud del Convenio y adoptando las medidas necesarias para aumentar la eficacia de las investigaciones y procedimientos penales. Cabe destacar que la utilización y aplicación del Convenio se ven facilitadas por la labor del Comité del Convenio sobre la Ciberdelincuencia (T-CY), establecido en virtud del artículo 46 del Convenio. Por otra parte, el

Convenio cuenta con el apoyo de los programas de fomento de capacidades a cargo de la Oficina del Programa de Lucha contra la Ciberdelincuencia del Consejo de Europa en Bucarest (Rumanía), que apoyan a todos los países del mundo en la aplicación del Convenio. Esta tríada de: i) las normas comunes del Convenio en materia de ciberdelincuencia; ii) un mecanismo sólido para la continua implicación de las Partes en el marco del T-CY, y iii) el énfasis sobre los programas de fomento de capacidades, ha contribuido significativamente a aumentar el alcance e impacto del Convenio.

9. En 2012, el T-CY, acorde con el mandato que le confiere el artículo 46, párrafo 1, del Convenio, acerca del "intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico" y de "la conveniencia de ampliar o enmendar el presente Convenio", estableció el Subgrupo Especial sobre Jurisdicción y Acceso Transfronterizo de Datos ("Grupo sobre el Acceso Transfronterizo"). En diciembre de 2014, el T-CY completó una evaluación de las disposiciones de asistencia mutua del Convenio sobre la Ciberdelincuencia y adoptó un conjunto de recomendaciones, incluidas algunas que se habrían de examinar en un nuevo protocolo del Convenio. Esa labor condujo a la creación en 2015 del Grupo de Trabajo sobre el Acceso de la Justicia Penal a la Evidencia Almacenada en Servidores en la Nube, incluso mediante la Asistencia Jurídica Mutua ("Grupo sobre Pruebas en la Nube").

10. En 2016, el Grupo sobre Pruebas en la Nube llegó a la conclusión de que, entre otras cosas, "la ciberdelincuencia, el número de dispositivos, servicios y usuarios (incluidos los de dispositivos y servicios móviles) y, con ellos, el número de víctimas, han alcanzado proporciones tales que solo una minúscula proporción de los delitos informáticos u otros delitos que implican pruebas electrónicas llegarán a registrarse e investigarse. La gran mayoría de las víctimas de la ciberdelincuencia no puede esperar que se haga justicia". Los principales retos identificados por el Grupo guardaban relación con "la computación en la nube, la territorialidad y la jurisdicción" y, por tanto, con las dificultades para obtener un acceso eficaz a las pruebas electrónicas o para su divulgación.

11. Al examinar las conclusiones del Grupo sobre Pruebas en la Nube, las Partes en el Convenio llegaron a la conclusión de que no era necesario modificar el Convenio ni prever una tipificación penal adicional mediante disposiciones de derecho penal sustantivo. Sin embargo, las Partes determinaron que era necesario adoptar medidas adicionales orientadas a mejorar la cooperación

y la capacidad de las autoridades de justicia penal para obtener pruebas electrónicas mediante la adopción de un segundo protocolo adicional, a fin de permitir una respuesta más eficaz de la justicia penal y de defender el estado de derecho.

Los trabajos preparatorios

12. La 17ª reunión plenaria del T-CY (8 de junio de 2017) aprobó el mandato para la preparación del presente Protocolo atendiendo a una propuesta elaborada por el Grupo sobre Pruebas en la Nube del T-CY. Decidió dar inicio a la redacción de este Protocolo por iniciativa propia en virtud del artículo 46, párrafo 1.c, del Convenio. El 14 de junio de 2017, el Secretario General Adjunto del Consejo de Europa informó de esta iniciativa del T-CY al Comité de Ministros (1289ª reunión de los Delegados de los Ministros).

13. Al principio, el mandato abarcaba el período comprendido entre septiembre de 2017 y diciembre de 2019; posteriormente el T-CY acordó prórrogas, primero hasta diciembre de 2020 y más tarde, hasta mayo de 2021.

14. En virtud de ese mandato, el T-CY creó un Pleno de Redacción del Protocolo (PDP) integrado por representantes de las Partes en el Convenio, y por Estados, organizaciones y órganos del Consejo de Europa que participan en el T-CY en calidad de observadores. En la preparación del proyecto de protocolo, el PDP contó con la asistencia de un Grupo de Redacción del Protocolo (PDG) integrado por expertos de las Partes en el Convenio. A su vez, el PDG creó varios subgrupos y grupos *ad hoc* que se ocuparon de disposiciones específicas.

15. Entre septiembre de 2017 y mayo de 2021, el T-CY organizó 10 sesiones plenarias de redacción, 16 reuniones del Grupo de Redacción y numerosas reuniones de subgrupos y grupos *ad hoc*. Gran parte de este Protocolo se preparó durante la pandemia de covid-19. Debido a las restricciones relacionadas con la covid-19, entre marzo de 2020 y mayo de 2021 tuvieron lugar más de 65 reuniones en formato virtual.

16. Los mencionados métodos de trabajo en sesiones plenarias, grupos de redacción y subgrupos y grupos *ad hoc* permitieron a los representantes y expertos de las Partes aportar importantes contribuciones a la redacción del presente Protocolo y elaborar soluciones innovadoras.

17. La Comisión de la Unión Europea participó en esa labor en nombre de los Estados Parte en el Convenio que eran miembros de la Unión Europea en virtud de un mandato de negociación otorgado por el Consejo de la Unión Europea el 6 de junio de 2019.

18. Una vez elaborados los proyectos de disposiciones, y tras su adopción provisional por el PDP, se procedió a publicar los proyectos de artículos y se invitó a las partes interesadas a formular observaciones.

19. El T-CY celebró seis rondas de consultas con las partes interesadas de la sociedad civil, el sector privado y con expertos en protección de datos: en julio de 2018, conjuntamente con la Conferencia Octopus sobre cooperación contra la ciberdelincuencia en Estrasburgo; en noviembre de 2018, en una reunión con expertos en protección de datos celebrada en Estrasburgo; en febrero de 2019 mediante la invitación formulada para la presentación de comentarios por escrito sobre los proyectos de artículos; en noviembre de 2019, en combinación con la Conferencia Octopus sobre cooperación contra la ciberdelincuencia que tuvo lugar en Estrasburgo; en diciembre de 2020, a través de la invitación para la presentación de comentarios escritos sobre nuevos proyectos de artículos, y en mayo de 2021 mediante presentaciones escritas y una reunión virtual que tuvo lugar el 6 de mayo de 2021.

20. Por otra parte, el T-CY realizó consultas con el Comité Europeo para los Problemas Criminales (CDPC) y el Comité Consultivo del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (T-PD) del Consejo de Europa.

21. La 24ª reunión plenaria del T-CY, celebrada el 28 de mayo de 2021, aprobó el proyecto de este Protocolo y decidió presentarlo al Comité de Ministros con vistas a su adopción.

Consideraciones de carácter sustantivo

22. En cuanto al fondo, el punto de partida de los trabajos sobre este Protocolo fue los resultados de la evaluación realizada por el T-CY de las disposiciones de asistencia mutua del Convenio en 2014, unido a los análisis y recomendaciones del Grupo sobre el Acceso Transfronterizo y del Grupo sobre Pruebas en la Nube del T-CY presentados en 2014 y 2017 respectivamente. Suscitaban especial preocupación los problemas de territorialidad y jurisdicción relacionados con las pruebas electrónicas, es decir, que los datos especificados necesarios en una investigación penal puedan estar almacenados en jurisdicciones múltiples, cambiantes o desconocidas ("en la nube"), por lo que son necesarias soluciones

que permitan obtener la divulgación de dichos datos de manera efectiva y eficiente a los efectos de investigaciones o procedimientos penales específicos.

23. Dada la complejidad de esas dificultades, quienes participaron en la redacción del presente Protocolo acordaron centrarse en las siguientes cuestiones específicas:

- En el momento en que se redactó este Protocolo, el método principal para obtener de otros Estados pruebas electrónicas de un delito penal eran las solicitudes de asistencia mutua, incluidos los instrumentos de asistencia mutua previstos en el Convenio. Sin embargo, la asistencia mutua no siempre es una forma eficaz de tramitar el número cada vez mayor de solicitudes destinadas a obtener pruebas electrónicas volátiles. Por lo tanto, se consideró necesario elaborar un mecanismo más ágil que permitiera emitir órdenes o solicitudes a los proveedores de servicios en otras Partes a fin de obtener información relativa a los abonados y datos sobre el tráfico.
- La información relativa a los abonados -por ejemplo, la que permite identificar al usuario de una cuenta específica de correo electrónico o de redes sociales, o de una dirección específica de Protocolo de Internet (IP) utilizada en la comisión de un delito- es el tipo de información que se solicita más frecuentemente en las investigaciones penales nacionales e internacionales relacionadas con la ciberdelincuencia y otros delitos que entrañan pruebas electrónicas. En muchos casos es imposible proceder con una investigación si no se dispone de esa información. En la mayoría de los casos, la obtención de información relativa a los abonados mediante la asistencia mutua no es eficaz y sobrecarga el sistema de asistencia mutua. La información relativa a los abonados suele estar en manos de los proveedores de servicios. Si bien el artículo 18 del Convenio ya aborda algunos aspectos referentes a la obtención de información relativa a los abonados directamente de los proveedores de servicios (véase la nota orientativa del T-CY sobre la interpretación del artículo 18), incluso ubicados en otras Partes, se estimó que era necesario incluir instrumentos complementarios que permitan obtener la divulgación de información relativa a los abonados directamente de un proveedor de servicios ubicado en otra Parte. Esos instrumentos redundarían en un aumento de la eficacia del proceso y también permitirían aliviar la presión sobre el sistema de asistencia mutua.
- Asimismo, en las investigaciones penales por lo general se desea obtener datos sobre el tráfico, y la rápida divulgación de los mismos puede ser

necesaria para rastrear el origen de una comunicación como punto de partida para reunir más pruebas o para identificar a un sospechoso.

- Asimismo, dado que muchas formas de delincuencia en línea se ven facilitadas por dominios creados o explotados con fines delictivos, es necesario identificar a la persona que ha registrado dicho dominio. Esa información está en manos de las entidades que prestan servicios de registro de nombres de dominio que, por lo general, son los registradores y los registros. Por consiguiente, es necesario contar con un marco eficaz para obtener esa información de las entidades pertinentes en otras Partes.
- En un caso de emergencia, en la que exista un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física, es necesario actuar con rapidez, ya sea mediante la prestación de asistencia mutua en caso de emergencia o recurriendo a los puntos de contacto de la Red 24/7 establecidos en el marco del Convenio (artículo 35).
- Además, deberían utilizarse más comúnmente y entre todas las Partes instrumentos de cooperación internacional de demostrada eficacia. Ya se han establecido medidas importantes como las videoconferencias o los equipos conjuntos de investigación en el marco de los tratados del Consejo de Europa (por ejemplo, el Segundo Protocolo Adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, STE nº 182) o en otros acuerdos bilaterales y multilaterales. Sin embargo, esos mecanismos no están disponibles de forma universal entre las Partes en el Convenio, por lo que el presente Protocolo pretende llenar ese vacío.
- El Convenio prevé la recogida e intercambio de información y pruebas para investigaciones o procedimientos penales específicos. Quienes participaron en la redacción reconocieron que el establecimiento, la ejecución y la aplicación de las facultades y los procedimientos relativos a las investigaciones y los procesos penales deben estar sujetos siempre a condiciones y salvaguardias que garanticen la protección adecuada de los derechos humanos y las libertades fundamentales. Por consiguiente, fue necesario incluir un artículo sobre condiciones y salvaguardias, similar al artículo 15 del Convenio. Asimismo, reconociendo que muchas Partes exigen protección de la intimidad y los datos personales para dar cumplimiento a sus obligaciones constitucionales e internacionales, quienes participaron en la redacción decidieron establecer en este Protocolo salvaguardias específicas en materia de protección de datos. Dichas salvaguardias de protección de datos complementan las obligaciones de muchas de las Partes en el Convenio, que también son

Partes del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108). El protocolo de modificación de dicho convenio (STE nº 223) se abrió a la firma en octubre de 2018, durante el proceso de redacción del presente Protocolo. Cabe señalar también que en el proceso de redacción del presente Protocolo participaron Partes no sujetas, en aquel entonces, a los instrumentos del Consejo de Europa en materia de protección de datos ni a las normas de protección de datos de la Unión Europea. Por consiguiente, se realizaron notables esfuerzos encaminados a garantizar un Protocolo equilibrado que refleje los diferentes sistemas jurídicos de Estados que probablemente serán Partes en el presente Protocolo y, al mismo tiempo, a respetar la importancia de velar por la protección de la vida privada y los datos personales, tal como exigen las constituciones y las obligaciones internacionales de otras Partes en el Convenio.

24. Quienes participaron en la redacción consideraron también otras medidas que, tras un examen a fondo, no se mantuvieron en este Protocolo. Dos de esas disposiciones, a saber, "las investigaciones encubiertas mediante un sistema informático" y "la ampliación de los registros", revestían un gran interés para las Partes, pero se estimó que las mismas requerían más trabajo, tiempo y consultas con las instancias correspondientes, por lo que no se consideraron viables en el plazo fijado para la elaboración del presente Protocolo. Quienes participaron en la redacción propusieron la adopción de un formato diferente para esas cuestiones, y la posibilidad de que sean recogidas en un instrumento jurídico separado.

25. En general, quienes participaron en la redacción consideraron que las disposiciones de este Protocolo aportarían un gran valor añadido desde el punto de vista operativo y también en cuanto a las políticas. El presente Protocolo aumentará significativamente la capacidad de las Partes para mejorar la cooperación entre ellas y entre las Partes y los proveedores de servicios y otras entidades, así como para obtener la divulgación de pruebas electrónicas a los efectos de investigaciones o procedimientos penales específicos. Por lo tanto, este Protocolo, al igual que el Convenio, tiene por objeto potenciar la capacidad de las autoridades encargadas de hacer cumplir la ley para combatir la ciberdelincuencia y otros delitos, respetando plenamente los derechos humanos y las libertades fundamentales, y hace hincapié en la importancia y el valor de una internet basada en la libre circulación de la información.

El Protocolo

26. Como se señala en el Preámbulo, el presente Protocolo tiene por objeto seguir mejorando: la cooperación en materia de ciberdelincuencia y la capacidad de las autoridades de justicia penal para reunir pruebas en formato electrónico de un delito penal a efectos de investigaciones o procedimientos penales específicos mediante instrumentos adicionales relacionados con una asistencia mutua más eficiente y otras formas de cooperación entre las autoridades competentes; la cooperación en casos de emergencia (es decir, en situaciones en las que existe un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física), y la cooperación directa entre las autoridades competentes y los proveedores de servicios y otras entidades que controlan o tienen en su poder la información pertinente. Por consiguiente, el presente Protocolo tiene por objeto complementar el Convenio y, en lo que respecta a las Partes en el mismo, el Primer Protocolo.

27. El presente Protocolo se divide en cuatro capítulos: I. Disposiciones comunes; II. Medidas de cooperación reforzada; III. Condiciones y salvaguardias; y IV. Disposiciones finales.

28. Las disposiciones comunes del capítulo I abarcan la finalidad y el ámbito de aplicación del presente Protocolo. Al igual que el Convenio, el presente Protocolo aborda investigaciones o procedimientos penales específicos, no sólo respecto de la ciberdelincuencia, sino de cualquier delito que entrañe pruebas en formato electrónico, también denominadas comúnmente "pruebas electrónicas" o "pruebas digitales". Asimismo, este capítulo dispone que las definiciones del Convenio son aplicables al presente Protocolo e incluye definiciones adicionales de términos utilizados con frecuencia en el presente Protocolo. Por otra parte, teniendo en cuenta que los requisitos lingüísticos en materia de asistencia mutua y otras formas de cooperación representan en muchos casos un obstáculo para la eficiencia de los procedimientos, se añadió un artículo sobre "lengua" que permite un enfoque más pragmático al respecto.

29. El capítulo II contiene los principales artículos sustantivos del presente Protocolo, en los que se describen los diversos métodos de cooperación de que disponen las Partes. Se aplican principios diferentes a cada tipo de cooperación. Debido a ello, fue necesario dividir ese capítulo en secciones: 1) principios generales aplicables al capítulo II; 2) procedimientos para mejorar la cooperación directa con proveedores y entidades de otras Partes que brindan servicios de registro de nombres de dominio; 3) procedimientos destinados a mejorar la cooperación internacional entre autoridades para la divulgación

de datos informáticos almacenados; 4) procedimientos relativos a la asistencia mutua en caso de emergencia, y 5) procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables.

30. El capítulo III establece las condiciones y salvaguardias. Precisan que las Partes aplicarán condiciones y salvaguardias similares a las del artículo 15 del Convenio también a las facultades y procedimientos del presente Protocolo. Además, ese capítulo incluye un conjunto pormenorizado de salvaguardias para la protección de los datos personales.

31. La mayoría de las disposiciones finales del capítulo IV son similares a las disposiciones finales estándar de los tratados del Consejo de Europa o estipulan que las disposiciones del Convenio sean aplicables al presente Protocolo. Sin embargo, el artículo 15, "Efectos del presente Protocolo"; el artículo 17, "Cláusula federal", y el artículo 23, "Consultas de las Partes y evaluación de la aplicación" difieren en diversos grados de las disposiciones análogas del Convenio. Este último artículo no sólo hace aplicable el artículo 46 del Convenio, sino que también establece que las Partes evaluarán periódicamente la aplicación efectiva de las disposiciones del presente Protocolo.

Comentario sobre los artículos del presente Protocolo

Capítulo I - Disposiciones comunes

Artículo 1 - Finalidad

32. La finalidad del presente Protocolo es complementar: i) el Convenio entre las Partes en el presente Protocolo, y ii) el Primer Protocolo entre las Partes en el Convenio que también son Partes en el presente Protocolo.

Artículo 2 - Ámbito de aplicación

33. El ámbito de aplicación general del presente Protocolo es el mismo que el del Convenio: las medidas del presente Protocolo se aplicarán, entre las Partes en el presente Protocolo, a investigaciones o procedimientos penales específicos relativos a delitos relacionados con sistemas y datos informáticos (es decir, los delitos contemplados en el artículo 14 del Convenio, párrafos 2.a y 2.b), así como a la obtención de pruebas en formato electrónico de un delito penal (artículo 14 del Convenio, párrafo 2.c) . Como se explica en los párrafos 141 y 243 del Informe explicativo del Convenio, esto significa que, cuando un delito se comete empleando un sistema informático, o cuando un delito común que no se ha cometido mediante la utilización

de un sistema informático (por ejemplo, un asesinato) involucra pruebas electrónicas, es de esperar que se pueda disponer de las facultades, los procedimientos y las medidas de cooperación que se definen en el presente Protocolo.

34. El párrafo 1.b establece que, como ocurre con las Partes en el Primer Protocolo que también son Partes en el presente Protocolo, éste también se aplica a investigaciones o procedimientos penales específicos relativos a los delitos tipificados con arreglo al Primer Protocolo. Las Partes en el presente Protocolo que no sean Partes en el Primer Protocolo no están obligadas a aplicar los términos del presente Protocolo a esos delitos.

35. En virtud del párrafo 2, cada Parte debe tener una base jurídica que permita cumplir las obligaciones establecidas en el presente Protocolo en caso de que sus tratados, leyes o acuerdos no incluyan ya tales disposiciones. Esto no convierte las disposiciones explícitamente discrecionales en disposiciones imperativas, y algunas disposiciones permiten formular declaraciones o reservas. Algunas Partes tal vez no requieran ninguna legislación de implementación para aplicar las disposiciones del presente Protocolo.

Artículo 3 - Definiciones

36. El párrafo 1 incorpora en el presente Protocolo las definiciones que figuran en los artículos 1 ("sistema informático", "datos informáticos", "proveedor de servicios" y "datos sobre el tráfico") y 18, párrafo 3 ("datos relativos al abonado") del Convenio. Quienes participaron en la redacción incluyeron esas definiciones del Convenio porque esos términos se utilizan en el texto de la parte dispositiva y en el Informe explicativo del presente Protocolo. Quienes participaron en la redacción también aspiraban a que se aplicaran igualmente a este Protocolo las explicaciones que figuran en el Informe explicativo del Convenio y en las notas orientativas (adoptadas por el T-CY) en relación con esos términos.

37. Las definiciones de los delitos y de otros términos incluidos en el texto del Convenio se aplicarán a los efectos de la cooperación entre las Partes en el presente Protocolo, y las definiciones de los delitos y de otros términos incluidos en el texto del Primer Protocolo se aplicarán a los efectos de la cooperación entre las Partes en el Primer Protocolo. Por ejemplo, el artículo 2, párrafo 1, establece que "las medidas descritas en el presente Protocolo se aplicarán... entre las Partes en el Convenio que sean Partes en el presente Protocolo, a las investigaciones o los procedimientos penales

concretos relativos a los delitos relacionados con sistemas y datos informáticos". Por consiguiente, al cooperar en el marco del presente Protocolo con respecto a los delitos relacionados con la pornografía infantil, se aplica la definición de "pornografía infantil" que figura en el párrafo 2 del artículo 9 del Convenio, y la definición de "menor" que figura en el párrafo 3 del artículo 9 del Convenio. Del mismo modo, entre las Partes en el Primer Protocolo que son Partes en el presente Protocolo, se aplica la definición de "material racista y xenófobo" que figura en el artículo 2 del Primer Protocolo. Las Partes en el presente Protocolo que no sean Partes en el Primer Protocolo no se comprometen a aplicar los términos o definiciones establecidos en el Primer Protocolo.

38. El párrafo 2 del artículo 3 incluye definiciones adicionales que se aplican al presente Protocolo y a la cooperación en el marco del presente Protocolo. En el párrafo 2.a, la "autoridad central" se define como la "autoridad o autoridades designadas en virtud de un tratado o acuerdo de asistencia mutua sobre la base de la legislación uniforme o recíproca en vigor entre las Partes interesadas o, en su defecto, la autoridad o autoridades designadas por una Parte en virtud del párrafo 2.a del artículo 27 del Convenio". En varios artículos del presente Protocolo se hace mención a las autoridades centrales, que son un canal de cooperación que las Partes ya utilizan y con el que están familiarizadas. Por lo tanto, las Partes que tienen tratados o acuerdos de asistencia mutua sobre la base de la legislación uniforme o recíproca en vigor deben recurrir a las autoridades centrales designadas en virtud de dichos tratados o acuerdos. Cuando no exista ningún tratado o acuerdo de esa índole entre las Partes interesadas, éstas deberán recurrir a la misma vía de autoridad central que utilizan actualmente conforme al artículo 27, párrafo 2.a, del Convenio. Aunque el término "autoridad central" no se emplea en todos los tratados o acuerdos de asistencia mutua basados en la legislación uniforme o recíproca en vigor entre las Partes, quienes participaron en la redacción aspiraban a que ese término se entienda en referencia a las autoridades de coordinación designadas en dichos tratados o acuerdos, independientemente del término que se emplee para denominarlas.

39. A menos que así se disponga específicamente en el presente Protocolo, el hecho de que las Partes recurran a esos canales de autoridad central a los efectos del presente Protocolo no significa que sean aplicables otras disposiciones de dichos tratados o acuerdos de asistencia mutua.

40. La definición de "autoridad competente" que figura en el párrafo 2.b se inspira en el párrafo 138 del Informe explicativo del Convenio. Como este

término se emplea frecuentemente en el presente Protocolo, la definición ha sido incluida en el texto de la parte dispositiva para facilitar la referencia.

41. En el párrafo 2.c, la "emergencia" se define como "una situación en la que existe un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física". Este término aparece en los artículos 9, 10 y 12. La definición de "emergencia" en el presente Protocolo tiene por objeto imponer un umbral considerablemente más elevado que el de las "circunstancias urgentes" que figura en el párrafo 3 del artículo 25 del Convenio. Esta definición ha sido redactada también para permitir a las Partes que consideren los diferentes contextos en los que se utiliza el término en el presente Protocolo, teniendo en cuenta al mismo tiempo las leyes y políticas aplicables de las Partes.

42. La definición de emergencia abarca situaciones en las que el riesgo es significativo e inminente, lo que significa que no incluye situaciones en las que el riesgo para la vida o la seguridad de la persona ya ha pasado, o es insignificante, o en las que pueda haber un riesgo futuro que no es inminente. La razón de esos requisitos de importancia e inminencia es que los artículos 9 y 10 imponen tanto a la Parte requerida como a la Parte requirente obligaciones que suponen personal numeroso y actividad intensiva para reaccionar de manera muy acelerada en casos de emergencia lo que, en consecuencia, exige dar mayor prioridad a las solicitudes de casos de emergencia que a otros casos importantes pero no tan urgentes, incluso si hubieran sido presentados con anterioridad. Las situaciones que entrañan "un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física" pueden implicar, por ejemplo, situaciones de toma de rehenes en las que existe un riesgo creíble de pérdida inminente de vidas, lesiones graves u otros daños comparables para la víctima; el abuso sexual persistente de un niño; situaciones apremiantes posteriores a un ataque terrorista en las que las autoridades tratan de determinar con quién se comunicaron los atacantes a fin de determinar si son inminentes nuevos ataques, y amenazas a la seguridad de infraestructuras vitales en las que existe un riesgo significativo e inminente para la vida o la seguridad de una persona física.

43. Como se explica en el artículo 10, párrafo 4 del presente Protocolo, y en el párrafo 154 de este Informe explicativo, relacionado con el artículo 9, la Parte requerida en virtud de esos artículos determinará si existe una "emergencia", con arreglo a la definición de este artículo.

44. En el párrafo 2.d, por "datos personales" se entiende la información relativa a una persona física identificada o identificable". Por "persona física

identificable" se entiende una persona que puede ser identificada, directa o indirectamente, por referencia, en particular, a un número de identificación o a uno o más factores específicos de su identidad física, fisiológica, mental, económica, cultural o social. La definición de "datos personales" que aparece en el Protocolo es coherente con la de otros instrumentos internacionales, como el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, modificado por su Protocolo adicional; las Directrices de Privacidad de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de 2013 que regulan la protección de la intimidad y los flujos transfronterizos de datos; el Reglamento General de Protección de Datos y la Directiva de la UE relativa a la aplicación de la Ley, y el Convenio de la Unión Africana sobre ciberseguridad y protección de los datos personales ("Convenio de Malabo").

45. Una persona no se considera "identificable" si su identificación requiere tiempo, esfuerzos o recursos poco razonables. Si bien un determinado tipo de información puede ser privativa de una persona en particular, y por lo tanto establecer por sí misma un vínculo con esa persona, otro tipo de información puede permitir la identificación solo cuando se combina con información personal o de identificación adicional. Por consiguiente, si la identificación de una persona basada en la vinculación con dicha información adicional requiere tiempo, esfuerzos o recursos poco razonables, la información en cuestión no constituye datos personales. El hecho de que una persona física pueda ser identificada o sea identificable, directa o indirectamente, depende de las circunstancias particulares en su contexto específico (y puede variar con el paso del tiempo debido a los avances tecnológicos o de otro tipo).

46. Los requisitos de protección de datos establecidos en el presente Protocolo no se aplican a los datos que no se consideran "datos personales", como la información anonimizada que no puede ser identificada nuevamente sin invertir tiempo, esfuerzos o recursos poco razonables.

Artículo 4 - Lengua

47. Este artículo establece un marco para los idiomas que pueden emplearse al dirigirse a las Partes y a los proveedores de servicios u otras entidades en virtud del presente Protocolo. Aun cuando en la práctica las Partes puedan trabajar en idiomas distintos de sus lenguas oficiales, esa posibilidad puede no estar prevista en el derecho interno o en los tratados. La finalidad de este artículo es brindar flexibilidad adicional en el marco del presente Protocolo.

48. Las traducciones inexactas o costosas de las solicitudes de asistencia mutua relativas a las pruebas electrónicas son una queja crónica que requiere atención urgente. Este impedimento erosiona los procesos legítimos para obtener datos y proteger la seguridad pública. Las mismas consideraciones se aplican al margen de la asistencia mutua tradicional, como ocurre cuando una Parte transmite una orden directamente a un proveedor de servicios en el territorio de otra Parte en virtud del artículo 7, o solicita que se dé efecto a una orden emitida en virtud del artículo 8. Si bien se espera que los sistemas de traducción automática mejoren, de momento son inadecuados. Por estas razones, el problema de la traducción figuraba repetidas veces en las propuestas sobre los artículos que se habrían de incluir en el presente Protocolo.

49. La traducción hacia y desde los idiomas menos comunes es un problema especial, ya que esas traducciones pueden retrasar mucho una solicitud o pueden ser efectivamente imposibles de obtener. También pueden llamar a engaño en aspectos cruciales, y su mala calidad puede hacer perder tiempo a ambas Partes. Con todo, el peso del coste y la dificultad de las traducciones recaen de forma desproporcionada en las Partes requirentes en los casos en que se hablan lenguas menos comunes.

50. Debido a esa carga desproporcionada, varias Partes no anglófonas pidieron que el inglés fuera obligatorio en el presente Protocolo. Señalaron que el inglés es un idioma utilizado habitualmente por los principales proveedores de servicios. Además, a medida que los datos transitan y se almacenan más ampliamente en el mundo y que más países participan en tareas de asistencia mutua, la traducción puede resultar incluso más engorrosa y poco práctica. Por ejemplo, dos Partes pueden utilizar idiomas menos comunes, estar distantes geográficamente y tener poco contacto. Si la Parte A necesita inesperadamente la asistencia de la Parte B, podría verse imposibilitada de encontrar un traductor para el idioma de B, o una eventual traducción podría resultar menos inteligible que una versión en inglés no nativo. Quienes participaron en la redacción hicieron especial hincapié en que, a fin de acelerar la asistencia, se debe hacer todo lo posible para que se acepten, en particular, las solicitudes en caso de emergencia emitidas en virtud del presente Protocolo en inglés o en un idioma compartido, en lugar de exigir la traducción en el idioma oficial de la Parte requerida.

51. Quienes participaron en la redacción de este Protocolo llegaron a la conclusión de que el inglés no debería ser obligatorio en el presente Protocolo. Algunas Partes tienen requisitos en materia de idiomas oficiales que excluyen esa posibilidad; muchas Partes comparten un idioma y no requieren el inglés;

y, en algunas Partes, es menos probable que puedan leer inglés los funcionarios en puntos alejados de las capitales que frecuentemente participan en la ejecución de las solicitudes.

52. Así, en la redacción del párrafo 1 se adoptó la formulación "una lengua aceptable para la Parte requerida o para la Parte notificada en virtud del artículo 7". Dicha Parte puede especificar los idiomas aceptables - por ejemplo, idiomas ampliamente hablados como el inglés, el español o el francés - incluso cuando éstos no estén previstos en su legislación interna o en los tratados.

53. Tal como se utiliza en el párrafo 1, por "las solicitudes, las órdenes y la información adjunta" se entenderá:

- en virtud del artículo 8, la solicitud (párrafo 3), la orden (párrafo 3.a), la información de apoyo (párrafo 3.b) y cualquier instrucción procesal especial (párrafo 3.c);
- en el caso de las Partes que requieran una notificación en virtud del artículo 7, párrafo 5, la orden (párrafo 3), la información complementaria (párrafo 4), y el resumen de los hechos (párrafo 5.a), y
- en virtud del artículo 9, la solicitud (párrafo 3).

Por "solicitudes" se entenderá también el contenido de las solicitudes presentadas en virtud de los artículos 10, 11 y 12, que incluye la documentación que forma parte de la solicitud.

54. En la práctica, algunos países pueden estar dispuestos a aceptar solicitudes y órdenes en un idioma distinto a los especificados en el derecho interno o en los tratados. Por ello, una vez al año, el T-CY realizará una encuesta informal sobre los idiomas aceptables para las solicitudes y órdenes. Las Partes pueden modificar su información en cualquier momento y todas las Partes serán informadas de cualquier cambio. Podrán declarar que sólo aceptan determinadas lenguas para formas específicas de asistencia. Los resultados de esa encuesta serán visibles para todas las Partes en el Convenio, no sólo para las Partes en el presente Protocolo.

55. Esta disposición pragmática demuestra la suma importancia que reviste acelerar la cooperación. Proporciona un fundamento jurídico para que una Parte acepte idiomas adicionales a los efectos del presente Protocolo.

56. En muchos casos, las Partes han suscrito tratados de asistencia mutua en los que se especifica el idioma o los idiomas en que deben presentarse las solicitudes en virtud de esos tratados. El presente artículo no interfiere con los términos de esos tratados u otros acuerdos entre las Partes. Además, se espera

que, a los efectos del presente Protocolo, "una lengua aceptable para la Parte requerida o para la Parte notificada en virtud del artículo 7" incluya cualquier idioma o idiomas especificados en esos tratados o acuerdos. Por consiguiente, en las solicitudes y notificaciones formuladas en virtud del presente Protocolo, la Parte requirente debería utilizar el idioma especificado en los tratados u otros acuerdos de asistencia mutua, a menos que la Parte requerida o notificada indique que también está dispuesta a aceptar esas solicitudes o notificaciones en otros idiomas.

57. La disposición de una Parte para aceptar otras lenguas se reflejará indicando al T-CY que está dispuesta a aceptar en otro idioma algunos o todos los tipos de solicitudes o notificación de órdenes en virtud del presente Protocolo.

58. El párrafo 2 determina la(s) lengua(s) que la Parte emisora utilizará para la presentación de las órdenes o solicitudes y de la información que las acompañe a los proveedores de servicios o a las entidades que prestan servicios de registro de nombres de dominio en el territorio de otra Parte a efectos de los artículos 7 y 6, respectivamente. Esta disposición tiene por objeto garantizar una cooperación rápida y una mayor certidumbre sin imponer una carga adicional a los proveedores de servicios o entidades que reciban órdenes o solicitudes de divulgación de datos. La primera opción, recogida en el párrafo 2.a, señala que la orden o solicitud puede presentarse en una lengua de la otra Parte en la que la entidad o el proveedor de servicios suele aceptar órdenes o solicitudes nacionales de sus propias autoridades en el marco de investigaciones o procedimientos penales específicos ("proceso nacional comparable"). En el caso de las Partes que tienen una o más lenguas oficiales, ello incluiría una de esas lenguas. La segunda opción, que figura en el párrafo 2.b, prevé que si un proveedor de servicios o una entidad acepta recibir órdenes o solicitudes en otra lengua, por ejemplo, la lengua de su sede, dichas órdenes y la información que las acompañe pueden presentarse en esa lengua. Como tercera opción, el párrafo 2.c dispone que, cuando la orden o solicitud y la información que las acompañe no hayan sido emitidas en una de las lenguas a que se refieren las dos opciones anteriores, deberán ir acompañadas de una traducción a una de ellas.

59. Tal como se utiliza en el párrafo 2, "las órdenes en virtud del artículo 7 y las solicitudes en virtud del artículo 6, así como cualquier información que las acompañe" se refiere a:

- en virtud del artículo 6, la solicitud (párrafo 3); y
- en virtud del artículo 7, la orden (párrafo 3) y la información complementaria (párrafo 4).

60. Cuando una Parte haya exigido notificación en virtud del artículo 7, la Parte requirente deberá estar dispuesta a enviar la orden y toda información complementaria en un idioma aceptable para la Parte que exija la notificación, sin perjuicio de que el proveedor de servicios acepte otros idiomas.

61. El T-CY también realizará esfuerzos informales para recopilar información sobre los idiomas en los que se presentarán las órdenes y solicitudes, así como la información que las acompañe, a los proveedores de servicios y a las entidades que prestan servicios de registro de nombres de dominio en virtud del artículo 4, párrafo 2, y los pondrá en conocimiento de las Partes como parte de la encuesta descrita en el párrafo 54 del Informe explicativo, *supra*.

Capítulo II - Medidas de cooperación reforzada

Sección 1 - Disposiciones generales aplicables al capítulo II

Artículo 5 - Principios generales aplicables al capítulo II

62. En el párrafo 1 del artículo 5 se aclara que, al igual que en el artículo 23 y en el artículo 25, párrafo 1, del Convenio, las Partes cooperarán, de conformidad con las disposiciones del capítulo II, "en la mayor medida posible". Este principio exige que las Partes brinden una amplia cooperación, y que reduzcan al mínimo los impedimentos para el flujo rápido y fluido de información y pruebas a nivel internacional.

63. Los párrafos 2 al 5 organizan las siete medidas de cooperación del presente Protocolo en cuatro secciones diferentes que van a continuación de la primera sección sobre los principios generales. Esas secciones están divididas en función de los tipos de cooperación deseada: La sección 2 abarca la cooperación directa con entidades privadas; la sección 3 contiene formas de cooperación internacional reforzada entre autoridades para la divulgación de los datos almacenados; la sección 4 prevé la asistencia mutua en caso de emergencia, y la sección 5 concluye con las disposiciones de cooperación internacional que deben aplicarse en ausencia de un tratado o acuerdo sobre la base de la legislación uniforme o recíproca en vigor entre las Partes interesadas. Esas secciones también están organizadas aproximadamente en una progresión que va desde las formas de asistencia en la investigación que habitualmente se solicitan al inicio de una investigación – con el fin de obtener la divulgación del registro de nombres de dominio e información relativa a los abonados - hasta l las solicitudes de datos sobre el tráfico, y los datos sobre el contenido , seguidos por las videoconferencias y los equipos

conjuntos de investigación, que son formas de asistencia que usualmente se solicitan en las fases posteriores de una investigación.

64. Esta sección sobre los principios generales aclara hasta qué punto cada medida se ve o no afectada por la existencia de un tratado o acuerdo de asistencia mutua sobre la base de la legislación uniforme o recíproca en vigor entre las Partes interesadas, es decir, la Parte requirente y la Parte requerida en el caso de la cooperación entre gobiernos, y la Parte que solicita la información y la Parte en cuyo territorio se encuentra la entidad privada que posee o controla dicha información cuando se trata de la cooperación directa en virtud de los artículos 6 y 7. Se entiende por "acuerdo sobre la base de la legislación uniforme o recíproca" los acuerdos "tales 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" (véase el Informe explicativo, párrafo 263, del Convenio). Las medidas de las Secciones 2 a 4 de este capítulo se aplican independientemente de que las Partes interesadas estén o no vinculadas mutuamente por un acuerdo o convenio de asistencia mutua aplicable sobre la base de la legislación uniforme o recíproca en vigor. Las disposiciones en materia de cooperación internacional que figuran en la sección 5 se aplican únicamente en ausencia de tales acuerdos o convenios, salvo que se disponga otra cosa.

65. Tal y como se describe en el párrafo 2 de este artículo, la sección 2 de este capítulo se compone del artículo 6, "Solicitud de información sobre el registro de nombres de dominio", y del artículo 7, "Divulgación de la información relativa a los abonados". Estos son los llamados artículos de "cooperación directa", que permiten a las autoridades competentes de una Parte interactuar directamente con entidades privadas –es decir, con entidades que prestan servicios de registro de nombres de dominio en el artículo 6, y con proveedores de servicios en el artículo 7– a efectos de investigaciones o procedimientos penales específicos. La sección 2 se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua sobre la base de la legislación uniforme o recíproca en vigor entre la Parte que solicita la información y la Parte en cuyo territorio se encuentra la entidad privada que posee o controla dicha información.

66. Como se indica en el párrafo 3 de este artículo, la sección 3 de este capítulo se compone del artículo 8, que lleva por título "Dar efecto a las órdenes de otra Parte para la producción acelerada de información relativa a los abonados y datos sobre el tráfico", y del artículo 9, "Divulgación acelerada de datos informáticos almacenados en caso de emergencia". Se trata de medidas

destinadas a mejorar la "cooperación internacional entre las autoridades", es decir, contempla la cooperación entre autoridades competentes, pero de naturaleza diferente a la cooperación internacional tradicional. La sección 3 se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua sobre la base de la legislación uniforme o recíproca en vigor entre las Partes requirente y requerida.

67. Como se señala en el párrafo 4 de este artículo, la sección 4 de este capítulo consiste en el artículo 10, "Asistencia mutua en caso de emergencia". A pesar de ser una disposición en materia de asistencia mutua, la asistencia mutua en caso de emergencia es un importante instrumento de cooperación para casos de emergencia que no está previsto expresamente en muchos tratados de asistencia mutua. Por lo tanto, quienes participaron en la redacción decidieron que esta sección debería aplicarse independientemente de que exista o no un acuerdo o convenio de asistencia mutua aplicable sobre la base de la legislación uniforme o recíproca en vigor entre las Partes interesadas. En cuanto a los procedimientos que rigen la asistencia mutua en caso de emergencia, existen dos posibilidades. Cuando las Partes interesadas están mutuamente vinculadas por un acuerdo o convenio de asistencia mutua aplicable sobre la base de la legislación uniforme o recíproca, la sección 4 se complementará con las disposiciones de dicho acuerdo, a menos que las Partes interesadas decidan de común acuerdo aplicar determinadas disposiciones del Convenio en lugar de las mismas (véase el artículo 10, párrafo 8, del presente Protocolo). Cuando las Partes interesadas no están mutuamente vinculadas por un acuerdo de asistencia mutua, las Partes aplicarán determinados procedimientos establecidos en los artículos 27 y 28 del Convenio que rigen la asistencia mutua en ausencia de un tratado (véase el artículo 10, párrafo 7 del presente Protocolo).

68. Como se indica en el párrafo 5 de este artículo, la sección 5 de este capítulo se compone del artículo 11, "Videoconferencia", y del artículo 12, "Equipos conjuntos de investigación e investigaciones conjuntas". Estas disposiciones son medidas de cooperación internacional, que se aplican únicamente cuando no existe un tratado o acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Partes requirente y requerida. Esas medidas no se aplicarán cuando exista tal tratado o acuerdo, con la salvedad de que el párrafo 7 del artículo 12 se aplicará independientemente de que exista o no ese tratado o acuerdo. Sin embargo, las Partes interesadas podrán decidir de común acuerdo aplicar las disposiciones de la sección 5 en lugar de un tratado o acuerdo existente, a menos que ello esté prohibido por los términos del tratado o acuerdo.

69. El párrafo 6 se inspira en el artículo 25, párrafo 5, del Convenio, por lo que el párrafo 259 del Informe explicativo del Convenio también es válido en este caso: "Cuando la Parte requerida se permite exigir la doble tipificación penal como condición para la prestación de asistencia ... se considerará que existe doble tipificación constitutiva del delito por el cual se pide la asistencia si fuera 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 a fin de garantizar que las Partes requeridas no adoptasen 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 haya 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 doble tipificación penal, ésta debería aplicarse de manera flexible que facilite la concesión de la ayuda."

70. El párrafo 7 establece que "[l]as disposiciones de este capítulo no restringen la cooperación entre las Partes, o entre las Partes y los proveedores de servicios u otras entidades, a través de otros acuerdos, convenios, prácticas o leyes nacionales aplicables." Esto significa que el Protocolo no elimina ni restringe ninguna cooperación entre las Partes o entre las Partes y las entidades privadas que esté disponible de otro modo, ya sea a través de acuerdos, convenios, leyes internas o incluso prácticas informales aplicables. Quienes participaron en la redacción tenían la intención de ampliar, no de restringir, los instrumentos disponibles para los profesionales encargados de hacer cumplir la ley a la hora de obtener información o pruebas para investigaciones o procedimientos penales específicos. Quienes participaron en la redacción reconocieron que, en determinadas situaciones, los mecanismos existentes, como la asistencia mutua, pueden ser los más adecuados para los profesionales. Sin embargo, en otras situaciones, los instrumentos creados por el presente Protocolo pueden ser más eficaces o preferibles. Por ejemplo, si una autoridad competente necesita datos sobre el contenido que no tienen carácter de emergencia, es probable que prefiera utilizar una solicitud tradicional de asistencia mutua en virtud de un tratado bilateral o en virtud del artículo 27 del Convenio, según proceda, porque el Protocolo no contiene disposiciones para obtener datos sobre el contenido cuando no se trata de un caso de emergencia. Sin embargo, si necesitara información relativa a los abonados, podría optar por recurrir al artículo 7 del Protocolo para emitir una orden directamente a un proveedor de servicios.

71. Por último, varias disposiciones del capítulo II y de otras partes del Protocolo permiten la imposición de restricciones o condiciones de utilización, como la confidencialidad. Cuando, de conformidad con las disposiciones del presente Protocolo, la recepción de las pruebas o la información que se desea obtener está sujeta a tal restricción o condición de utilización, los negociadores reconocieron excepciones que están implícitas en el texto. En primer lugar, como medida de protección de los derechos humanos y las libertades, de conformidad con el artículo 13, en virtud de los principios jurídicos fundamentales de muchos Estados, si el material facilitado a la Parte receptora es considerado por ésta como exculpatorio de un acusado, debe revelarse a la defensa o a una autoridad judicial. Este principio se entiende sin perjuicio del texto del artículo 12, párrafo 6.b, y del párrafo 215 del Informe explicativo, que podrán aplicarse cuando las Partes hayan establecido un equipo conjunto de investigación. Quienes participaron en la redacción entendieron que, en tales casos, la Parte receptora notificaría a la Parte transferente antes de divulgar la información y, si así se lo solicita, consultaría con la Parte transferente. En segundo lugar, cuando se ha impuesto una restricción de utilización con respecto al material recibido en virtud de este Protocolo que se prevé utilizar en una causa, el juicio (incluidas las revelaciones durante los procedimientos judiciales previos al juicio) es normalmente un proceso público. Una vez hecho público en el juicio, el material ha pasado al dominio público. En esas situaciones, no es posible garantizar la confidencialidad de la investigación ni del procedimiento para el que se solicitó el material. Esas excepciones son similares a las relacionadas con la aplicación del artículo 28, párrafo 2, del Convenio, tal como se explica en el párrafo 278 del Informe explicativo del Convenio. Por último, el material puede destinarse a otro fin cuando se haya obtenido el consentimiento previo de la Parte transferente.

Sección 2 - Procedimientos para mejorar la cooperación directa con proveedores y entidades de otras Partes

Artículo 6 - Solicitud de información sobre el registro de nombres de dominio

72. El artículo 6 establece un procedimiento que prevé la cooperación directa entre las autoridades de una Parte y una entidad que presta servicios de registro de nombres de dominio en el territorio de otra Parte a fin de obtener información sobre los registros de nombres de dominio de Internet. Al igual que ocurre con el artículo 7, el procedimiento se basa en las conclusiones del Grupo

de Pruebas en la Nube del Comité del Convenio sobre la Ciberdelincuencia, en reconocimiento de la importancia del acceso transfronterizo oportuno a las pruebas electrónicas en investigaciones o procedimientos penales específicos, en vista de las dificultades que plantean los procedimientos existentes para la obtención de pruebas electrónicas.

73. El procedimiento también reconoce el modelo actual de gobernanza de internet, que se basa en el desarrollo de políticas consensuadas entre las múltiples partes interesadas. Esas políticas están basadas normalmente en el derecho contractual. El procedimiento establecido en este artículo tiene por objeto complementar esas políticas a los efectos del presente Protocolo, es decir, a los fines de investigaciones o procedimientos penales específicos. La obtención de los datos de registro de los nombres de dominio suele ser indispensable como primer paso en muchas investigaciones penales, y también para determinar a quién dirigir las solicitudes de cooperación internacional.

74. Muchas formas de ciberdelincuencia se ven facilitadas por delincuentes que crean y explotan dominios con fines maliciosos e ilícitos. Por ejemplo, un nombre de dominio puede servir de plataforma para la propagación de programas maliciosos (*malware*), redes de bots, suplantación de identidad (*phishing*) y actividades similares, fraude, distribución de material de abuso infantil y otros fines delictivos. Por lo tanto, el acceso a la información sobre la persona física o jurídica que registró un dominio (el "titular registral") es fundamental para identificar a un sospechoso en una investigación o procedimiento penal específico. Mientras que en el pasado los datos de registro de nombres de dominio estaban a disposición del público, el acceso a parte de la información está ahora restringido, lo que afecta a las autoridades judiciales y policiales en sus tareas de orden público.

75. La información sobre el registro de nombres de dominio está en manos de entidades que prestan servicios de registro de nombres de dominio. Entre ellas figuran las organizaciones que venden nombres de dominio al público ("registradores"), así como los operadores de registros regionales o nacionales que mantienen bases de datos autorizadas ("registros") de todos los nombres de dominio registrados para un dominio de nivel superior y que aceptan solicitudes de registro. En ciertos casos, dicha información puede incluir datos personales y puede estar protegida por la normativa de protección de datos de la Parte donde se encuentra la entidad respectiva que presta los servicios de registro de nombres de dominio (el registrador o el registro) o en la que se encuentra la persona a quien se refieren los datos.

76. La finalidad del artículo 6 es establecer un marco eficaz y eficiente para obtener información que permita identificar al titular de un nombre de dominio o ponerse en contacto con él. La forma en que se aplique depende de las consideraciones jurídicas y políticas respectivas de las Partes. Este artículo tiene por objeto complementar las políticas y prácticas actuales y futuras de gobernanza de internet.

Párrafo 1

77. De conformidad con el párrafo 1, cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes a emitir solicitudes directamente a una entidad que preste servicios de registro de nombres de dominio en el territorio de otra Parte, es decir, sin que sea necesario que las autoridades del territorio en el que se encuentra la entidad actúen como intermediarias. El párrafo 1 brinda flexibilidad a las Partes en cuanto al formato en que se presentarán las solicitudes, ya que el formato depende de las consideraciones jurídicas y políticas respectivas de las Partes. Una Parte podría recurrir a procedimientos disponibles en su legislación nacional, incluida la emisión de una orden; sin embargo, a los efectos del artículo 6, dicha orden se considerará una solicitud no vinculante. Por consiguiente, la forma de la solicitud o los efectos que produzca con arreglo al derecho interno de la Parte requirente no afectarían al carácter voluntario de la cooperación internacional en virtud del presente artículo y, si la entidad no divulga la información solicitada, sería aplicable el párrafo 5.

78. La formulación del artículo 6, párrafo 1, es lo suficientemente amplia como para reconocer la posibilidad de emitir dicha solicitud, y de obtener la información, a través de una interfaz, un portal u otra herramienta técnica puesta a disposición por las organizaciones. Por ejemplo, una organización puede ofrecer una interfaz o una herramienta de búsqueda para facilitar o agilizar la divulgación de la información de registro del nombre de dominio tras recibir una solicitud. Empero, en lugar de adaptar este artículo a un portal o interfaz concreto, en el artículo se emplean términos tecnológicamente neutros para permitir su adaptación a medida que evolucione la tecnología.

79. Como se prevé en el artículo 2, una solicitud con arreglo al párrafo 1 sólo podrá emitirse a efectos de investigaciones o procedimientos penales específicos. El término "autoridad competente", definido en el artículo 3, párrafo 2.b, se refiere a una "autoridad judicial, administrativa u otra autoridad encargada de hacer cumplir la ley que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas en virtud del

presente Protocolo". Por "entidad que preste servicios de registro de nombres de dominio" se entiende en la actualidad a los registradores y a los registros. Para tener en cuenta la situación actual y al mismo tiempo permitir su adaptación, en vista de la evolución con el tiempo de los modelos de negocio y de la arquitectura de la Internet, en este artículo se emplea el término más genérico de "entidad que presta servicios de registro de nombres de dominio".

80. Si bien la información necesaria para identificar al titular de un nombre de dominio, o para ponerse en contacto con él, suele ser almacenada por entidades que prestan servicios generales de registro de nombres de dominio en todo el mundo, por ejemplo "dominios de nivel superior genéricos" (gTLD), las Partes reconocieron que los nombres de dominio más específicos relacionados con entidades nacionales o regionales ("dominios de nivel superior de código de país" (ccTLD)) también pueden ser registrados por personas o entidades en otros países y pueden ser utilizados también por delincuentes. Por lo tanto, el artículo 6 no se limita a las entidades que proporcionan gTLD, ya que ambos tipos de servicios de registro de nombres de dominio – u otros servicios futuros de este tipo - pueden ser utilizados para perpetrar delitos informáticos.

81. La expresión " información... para identificar o ponerse en contacto con el titular de un nombre de dominio" se refiere a la información previamente disponible públicamente a través de las llamadas herramientas de búsqueda WHOIS, como el nombre, la dirección física, la dirección de correo electrónico y el número de teléfono del titular del nombre registrado. Algunas Partes pueden considerar que esa información es un subconjunto de la información relativa a los abonados, tal como se define en el artículo 18, párrafo 3 del Convenio. La información relativa al registro de nombres de dominio es una información básica que no permite extraer conclusiones precisas sobre la vida privada y los hábitos diarios de las personas. Por lo tanto, su divulgación puede ser menos intrusiva que la de otras categorías de datos.

Párrafo 2

82. Con arreglo al párrafo 2, cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para permitir que las entidades en su territorio que prestan servicios de registro de nombres de dominio puedan divulgar dicha información en respuesta a una solicitud en virtud del párrafo 1, sujeto a las condiciones razonables previstas en la legislación nacional, que en algunas Partes puede incluir condiciones relativas a la protección de datos. Al mismo tiempo, el artículo 14 limita la capacidad de rechazar las transferencias de datos en virtud de las normas de protección de datos aplicables a las

transferencias internacionales; los factores que figuran en el párrafo 83 fueron incluidos para facilitar el tratamiento conforme a reglas de protección de los datos. Esas medidas deben facilitar la divulgación de los datos solicitados de manera rápida y eficaz en la mayor medida posible.

83. Este artículo no exige a las Partes que promulguen legislación que obligue a esas entidades a responder a una solicitud de una autoridad de otra Parte. Por lo tanto, la entidad que ofrece servicios de registro de nombres de dominio puede tener que determinar si debe divulgar la información solicitada. A fin de contribuir a esa determinación, el presente Protocolo ofrece salvaguardias que deberían facilitar la capacidad de las entidades para responder sin dificultad a las solicitudes en virtud de este artículo, tales como:

- el presente Protocolo establece o exige a las Partes que proporcionen una base jurídica para las solicitudes;
- este artículo exige que la solicitud emane de una autoridad competente (artículo 6, párrafos 1 y 3.a, y párrafos 79 y 84 del Informe explicativo);
- este Protocolo establece que la solicitud se hará a efectos de investigaciones o procedimientos penales específicos (artículo 2);
- este artículo exige que la solicitud contenga una declaración en el sentido de que la necesidad de la información obedece a su relevancia para una investigación o procedimiento penal específico y que la información será utilizada únicamente para dicha investigación o procedimiento penal específico (artículo 6, párrafo 3.c);
- el presente Protocolo establece garantías para el tratamiento de los datos personales divulgados y transferidos en virtud de dichas solicitudes a través del artículo 14;
- la información que debe divulgarse es limitada y no permitiría extraer conclusiones precisas sobre la vida privada de las personas;
- se puede esperar o exigir que las entidades cooperen en virtud de acuerdos contractuales con la Corporación de Asignación de Nombres y Números de Internet (ICANN).

Párrafo 3

84. El párrafo 3 de este artículo especifica la información que, como mínimo, deberá facilitar la autoridad que emita una solicitud con arreglo al párrafo 1 del presente artículo. Esa información es especialmente relevante para la ejecución de la solicitud por parte de la entidad que presta servicios de registro de nombres de dominio. La solicitud deberá incluir:

a. la fecha de emisión de la solicitud y la identidad y los datos de contacto de la autoridad competente que emite la solicitud (párrafo 3.a), (véase el párrafo 79 del Informe explicativo);

b. el nombre de dominio acerca del que se solicita información y una lista pormenorizada de la información que se solicita, incluidos elementos de datos concretos como el nombre, la dirección física, la dirección de correo electrónico o el número de teléfono del registrante (párrafo 3.b)

c. una declaración en la que se indique que la solicitud se emite en virtud del presente Protocolo; al formular esa declaración, la Parte atestigua que la solicitud se ajusta a lo dispuesto en el presente Protocolo (párrafo 3.c). Asimismo, la Parte requirente confirma en esa declaración que la información es "necesaria" debido a su pertinencia para una investigación o procedimiento penal específico y que la información se utilizará solamente para esa investigación o procedimiento penal específico. Por lo que se refiere a los países europeos, la información "necesaria" -es decir, necesaria y proporcionada- para una investigación o procedimiento penal debe estar acorde con los principios del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, su jurisprudencia aplicable y la legislación y jurisprudencia nacionales. Esas fuentes estipulan que el poder o procedimiento deberá ser proporcional a la naturaleza y las circunstancias del delito (véase el párrafo 146 del Informe explicativo del Convenio sobre la Ciberdelincuencia). Otras Partes aplicarán principios conexos de su legislación, como los principios de pertinencia (es decir, que las pruebas que se piden deben ser pertinentes para la investigación o el enjuiciamiento). Las Partes deben evitar las solicitudes amplias de divulgación de información sobre nombres de dominio, a menos que sean necesarias para la investigación o el procedimiento penal específico;

d. el momento y la forma en que se divulgará la información y cualquier otra instrucción procesal especial (párrafo 3.d). Por "instrucción procesal especial " se entenderá toda solicitud de confidencialidad, incluida la solicitud de no divulgación de la solicitud al autor del registro o a otros terceros. Si es necesaria confidencialidad para evitar una divulgación prematura del asunto, ello deberá indicarse en la solicitud. En algunas Partes, la confidencialidad de la solicitud se mantendrá por imperativo legal, mientras que en otras Partes no es necesariamente así. Por lo tanto, cuando sea necesaria la confidencialidad, se alienta a las Partes a que examinen la información disponible públicamente y a que soliciten orientación a otras Partes en relación con la legislación aplicable, así como con las políticas de las entidades que prestan servicios de registro

de nombres de dominio en lo que respecta a la información relativa a los abonados/registrantes, antes de presentar a la entidad una solicitud en virtud del párrafo 1. Además, las instrucciones procesales especiales podrán incluir la especificación del canal de transmisión más adecuado a las necesidades de la autoridad.

85. El párrafo 3 no exige que en la solicitud se incluya una exposición de los hechos, en vista de que esa información es confidencial en la mayoría de las investigaciones penales y no puede ser divulgada a un particular. Sin embargo, la entidad que recibe una solicitud en virtud de este artículo puede necesitar alguna información adicional que le permita tomar una decisión positiva con respecto a la solicitud. Por lo tanto, la entidad puede pedir más información cuando no pueda ejecutar la solicitud de otro modo.

Párrafo 4

86. La finalidad del párrafo 4 es fomentar la utilización de medios electrónicos cuando resulte aceptable para la entidad que presta servicios de registro de nombres de dominio, ya que los medios electrónicos son casi siempre los medios de comunicación más rápidos y eficientes. En consecuencia, si es aceptable para la entidad que presta servicios de registro de nombres de dominio, una Parte puede presentar una solicitud a la entidad en formato electrónico, por ejemplo, utilizando correo electrónico, portales electrónicos u otros medios. Si bien se supone que las entidades prefieren recibir las solicitudes en ese formato, no es una obligación utilizar solamente ese formato. Como se prevé en otros artículos del presente Protocolo que permiten órdenes o solicitudes en formato electrónico (como los artículos 7, 8 y otros), pueden exigirse niveles adecuados de seguridad y autenticación. Las Partes y las entidades podrán decidir por sí mismas si se dispone de canales o medios seguros para la transmisión y la autenticación o si pueden ser necesarias protecciones de seguridad especiales (incluido el cifrado) en un caso particular sensible.

Párrafo 5

87. Si bien esta disposición se refiere a las "solicitudes" y no a las "órdenes" obligatorias de divulgación de los datos de registro de los nombres de dominio, se espera que la entidad requerida pueda divulgar la información solicitada en virtud de esta disposición cuando se hayan cumplido las condiciones aplicables. Si la entidad no divulga la información solicitada, podrían considerarse otros mecanismos para obtener la información, dependiendo de las circunstancias. Por lo tanto, el párrafo 5 prevé la celebración de consultas entre las partes interesadas a fin de obtener información adicional y determinar los

mecanismos disponibles, por ejemplo, para mejorar la cooperación futura. A fin de facilitar las consultas, el párrafo 5 también dispone que una Parte requirente podrá pedir más información a una entidad. Se alienta a las entidades a que expliquen las razones por las que no divulgan los datos solicitados en respuesta a una petición de ese tipo.

Párrafo 6

88. El párrafo 6 exige que, en el momento de la firma del presente Protocolo, o al depositar su instrumento de ratificación, aceptación o aprobación, o en cualquier otro momento, las Partes designen una autoridad para los fines de consultas con arreglo al párrafo 5. La designación de un punto de contacto en la Parte donde se encuentra la entidad ayudará a la Parte requirente a determinar rápidamente qué medidas están disponibles para obtener los datos solicitados, en caso de que la entidad se niegue a ejecutar una solicitud directa realizada en virtud del artículo 6.

Párrafo 7

89. El párrafo 7 se explica por sí mismo y dispone que el Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de las autoridades designadas con arreglo al párrafo 6 y que cada Parte se asegurará de que los datos que haya facilitado para el registro sean correctos en todo momento.

Artículo 7 - Divulgación de la información relativa a los abonados

90. El artículo 7 establece un procedimiento que prevé la cooperación directa entre las autoridades de una Parte y un proveedor de servicios en el territorio de otra Parte con el fin de obtener información relativa a los abonados. El procedimiento se basa en las conclusiones del Grupo sobre Pruebas en la Nube del TC-Y y en la nota orientativa sobre la interpretación del artículo 18 del Convenio, en que se reconoce la importancia del acceso transfronterizo oportuno a las pruebas electrónicas en investigaciones o procedimientos penales concretos, en vista de los problemas que plantean los procedimientos existentes para obtener pruebas electrónicas de los proveedores de servicios en otros países.

91. En la actualidad, un número cada vez mayor de investigaciones o procedimientos penales requieren el acceso a pruebas electrónicas de proveedores de servicios en otros países. Incluso en el caso de delitos de carácter totalmente nacional -es decir, cuando el delito, la víctima y el autor se encuentran todos en

el mismo país que la autoridad investigadora- las pruebas electrónicas pueden estar en poder de un proveedor de servicios en el territorio de otro país. En muchas situaciones, las autoridades que investigan un delito pueden verse obligadas a recurrir a procedimientos de cooperación internacional, como la asistencia mutua, que no siempre pueden prestar asistencia con la rapidez y eficacia suficientes para satisfacer las necesidades de la investigación o el procedimiento, debido al volumen cada vez mayor de solicitudes de pruebas electrónicas.

92. La información relativa a los abonados es la información solicitada más frecuentemente en las investigaciones penales relacionadas con la ciberdelincuencia y otros tipos de delitos para los que son necesarias pruebas electrónicas. Este tipo de información incluye la identidad de un abonado concreto a un servicio, su dirección, e información similar identificada en el artículo 18, párrafo 3, del Convenio. No permite sacar conclusiones precisas sobre la vida privada y los hábitos cotidianos de las personas concernidas, lo que significa que su divulgación puede tener un menor grado de intrusión en comparación con la divulgación de otras categorías de datos.

93. La información relativa a los abonados se define en el artículo 18, párrafo 3 del Convenio (incorporado en el artículo 3, párrafo 1 del presente Protocolo) como "toda información contenida en forma de datos informáticos o de cualquier otra forma que posea el proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de servicios"; c) cualquier otra información sobre el lugar de la instalación de los equipos de comunicación, disponible sobre la base del acuerdo o contrato de prestación de servicios (véase también el Informe explicativo del Convenio sobre la Ciberdelincuencia, párrafos 177 a 183). La información necesaria para identificar a un abonado de un servicio puede incluir información específica sobre la dirección del Protocolo de Internet (IP) - por ejemplo, la dirección IP utilizada en el momento en que se creó la cuenta, la dirección IP de inicio de sesión más reciente o las direcciones IP de inicio de sesión utilizadas en un momento determinado. En algunas Partes esta información se trata como datos sobre el tráfico por varias razones, entre ellas que se considera que está relacionada con la transmisión

de una comunicación. En consecuencia, el párrafo 9.b del artículo 7 establece una reserva para algunas Partes.

94. Aunque el artículo 18 del Convenio ya aborda algunos aspectos de la necesidad de un acceso rápido y eficiente a las pruebas electrónicas solicitadas a los proveedores de servicios, no ofrece por sí solo una solución completa a este problema, ya que dicho artículo se aplica en un conjunto más limitado de circunstancias. Específicamente, el artículo 18 del Convenio se aplica cuando un proveedor de servicios se encuentra "en el territorio" de la Parte emisora (véase el artículo 18, párrafo 1.a del Convenio) u "ofrece sus servicios" en la Parte emisora (véase el artículo 18, párrafo 1.b del Convenio). Habida cuenta de los límites del artículo 18 y de los problemas que planteaba la asistencia mutua, se consideró importante establecer un mecanismo complementario que permitiera un acceso transfronterizo más eficaz a la información necesaria para investigaciones o procedimientos penales específicos. En consecuencia, el alcance del artículo 7 del presente Protocolo va más allá del ámbito de aplicación del artículo 18 del Convenio al permitir que una Parte emita ciertos tipos de órdenes a proveedores de servicios en el territorio de otra Parte. Las Partes reconocieron que, si bien tales órdenes directas de las autoridades de una Parte a los proveedores de servicios ubicados en otra Parte son deseables para obtener un acceso rápido y eficiente a la información, no se debe permitir que una Parte utilice todos los mecanismos de ejecución disponibles en su legislación nacional para la ejecución de esas órdenes. Por esa razón, la ejecución de esas órdenes en los casos en que el proveedor no divulgue la información especificada relativa al abonado se ve limitada de la manera establecida en el párrafo 7 del artículo 7. Este procedimiento prevé salvaguardias para tener en cuenta los requisitos especiales que se deriven de la cooperación directa entre las autoridades de una Parte con los proveedores de servicios ubicados en otra Parte.

95. Como se refleja en el artículo 5, párrafo 7, este artículo se entiende sin perjuicio de la capacidad de las Partes para ejecutar las órdenes emitidas en virtud del artículo 18 o de cualquier otra forma permitida por el Convenio, ni prejuzga la cooperación (incluida la cooperación espontánea) entre las Partes, o entre las Partes y los proveedores de servicios, a través de otros acuerdos, convenios, prácticas o normativas nacionales aplicables.

Párrafo 1

96. El párrafo 1 exige que las Partes adopten las medidas necesarias para que sus autoridades competentes estén facultadas para emitir una orden que se presentará a un proveedor de servicios en el territorio de otra Parte a fin

de obtener la divulgación de la información relativa a los abonados. La orden sólo podrá emitirse para la información relativa a los abonados especificada y almacenada.

97. El párrafo 1 también incluye el requisito de que las órdenes sólo pueden emitirse y presentarse en el contexto de "investigaciones o procedimientos penales específicos" de la Parte emisora, tal como se define esa expresión en el artículo 2 del presente Protocolo. Como restricción adicional, las órdenes también pueden emitirse únicamente para la información que sea "necesaria para" esa investigación o procedimiento. En lo referente a los países europeos, la información que se necesita - es decir, necesaria y proporcionada - para una investigación o procedimiento penal debe estar acorde con los principios del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y las Libertades Fundamentales de 1950, su jurisprudencia aplicable y la legislación y jurisprudencia nacionales. Esas fuentes estipulan que la facultad o el procedimiento debe ser proporcional a la naturaleza y las circunstancias del delito (véase el párrafo 146 del Informe explicativo del Convenio). Otras Partes aplicarán principios conexos de su legislación, como los principios de pertinencia (es decir, que las pruebas solicitadas por una orden deben ser pertinentes para la investigación o el enjuiciamiento) y los referentes a evitar órdenes excesivamente amplias para la divulgación de información relativa a los abonados. Esta restricción reafirma el principio ya establecido en el artículo 2 del presente Protocolo y en el párrafo 1 del artículo 7, que restringe la medida a investigaciones y procedimientos penales específicos, y que estipula que las disposiciones no pueden utilizarse para la producción masiva o a granel de datos (véase también el párrafo 182 del Informe explicativo del Convenio).

98. Tal como se define en el párrafo 2.b del artículo 3, el término "autoridad competente" se refiere a una autoridad judicial, administrativa u otra autoridad encargada de hacer cumplir la ley que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de las medidas previstas en virtud del presente Protocolo. Se contempla el mismo criterio a efectos del procedimiento de cooperación directa en este artículo. En consecuencia, el ordenamiento jurídico interno de una Parte determinará qué autoridad se considera competente para emitir una orden. Si bien la Parte emisora determina cuál de sus autoridades puede emitir la orden, el artículo 7 establece una salvaguardia en el párrafo 5 con arreglo a la cual la Parte receptora puede exigir que una autoridad designada revise las órdenes emitidas en virtud de este artículo y tenga la competencia para frenar la cooperación directa, como se describe más adelante.

99. En el artículo 7, el término "un proveedor de servicios en el territorio de otra Parte" precisa que el proveedor de servicios deberá estar físicamente presente en la otra Parte. En virtud de este artículo, el mero hecho de que, por ejemplo, un proveedor de servicios haya establecido una relación contractual con una empresa de una Parte, pero el propio proveedor de servicios no esté físicamente presente en esa Parte, no significa que el proveedor de servicios está "en el territorio" de esa Parte. El párrafo 1 exige, además, que los datos estén en posesión o bajo el control del proveedor de servicios.

Párrafo 2

100. El párrafo 2 del artículo 7 establece que las Partes están obligadas a adoptar las medidas necesarias para que los proveedores de servicios de su territorio puedan responder a una orden emitida por una autoridad competente de otra Parte de conformidad con el párrafo 1. Habida cuenta de las diferencias en los sistemas jurídicos nacionales, las Partes pueden aplicar diferentes medidas con el fin de establecer un procedimiento para que la cooperación directa transcurra de manera eficaz y eficiente. Ello puede ir desde la eliminación de los obstáculos legales para que los proveedores de servicios respondan a una orden hasta el establecimiento de una base afirmativa que obligue a los proveedores de servicios a responder a una orden de una autoridad de otra Parte de manera eficaz y eficiente. Cada Parte deberá garantizar que los proveedores de servicios puedan cumplir legalmente las órdenes previstas en el artículo 7 de una manera que brinde seguridad jurídica, de modo que los proveedores de servicios no incurran en responsabilidad jurídica por el mero hecho de haber cumplido de buena fe con una orden emitida en virtud del párrafo 1, que una Parte haya declarado (de conformidad con el artículo 7, párrafo 3.b) haber sido emitida en virtud del presente Protocolo. Esto no excluye la responsabilidad por otras razones distintas al cumplimiento de la orden, por ejemplo, el incumplimiento de cualquier requisito legal aplicable que obligue a un proveedor de servicios a mantener niveles adecuados de seguridad de la información almacenada. La forma de aplicación depende de las respectivas consideraciones legales y políticas de las Partes. En el caso de las Partes que tienen requisitos en materia de protección de datos, ello incluiría proporcionar una base clara para el tratamiento de los datos personales. En vista de los requisitos adicionales establecidos en las leyes de protección de datos para autorizar eventuales transferencias internacionales de la información relativa a los abonados que ha sido solicitada, el presente Protocolo refleja el importante interés público de esta medida de cooperación directa e incluye en el artículo 14 las salvaguardias necesarias a tal efecto.

101. Como se ha explicado anteriormente, el ordenamiento jurídico interno de una Parte determinará cuál autoridad se considera competente para emitir una orden. Algunas Partes estimaron necesario contar con una salvaguardia adicional que permita proceder a un nuevo examen de la legalidad de la orden (véase, por ejemplo, el párrafo 98 *supra*) en vista del carácter directo de la cooperación. Si bien la Parte emisora determina cuál de sus autoridades está autorizada a emitir la orden, el párrafo 2.b permite a las Partes formular una declaración en la que se indique que "la orden en virtud del párrafo 1 debe ser emitida por un fiscal u otra autoridad judicial, o bajo su supervisión, o de lo contrario ser emitida bajo una supervisión independiente". La Parte que haga uso de esa declaración deberá aceptar una orden emitida por cualquiera de las autoridades enumeradas, o bajo su supervisión.

Párrafo 3

102. El párrafo 3 del artículo 7 especifica la información que, como mínimo, deberá suministrar una autoridad que emita una orden de conformidad con el párrafo 1 de este artículo, aunque una Parte emisora puede optar por incluir información adicional en su orden para facilitar la tramitación o porque su derecho interno exige información adicional. La información especificada en el párrafo 3 es particularmente relevante para la ejecución de la orden por parte del proveedor de servicios, así como para la posible participación de la autoridad de la Parte en la que se encuentra el proveedor de servicios con arreglo al párrafo 5. La orden deberá incluir el nombre de la autoridad emisora y la fecha de emisión de la orden; información que permita identificar al proveedor de servicios; el delito o delitos que son objeto de la investigación o el procedimiento penal; la autoridad que solicita la información específica relativa al abonado, y una descripción detallada de la información específica relativa al abonado que se desea obtener. Asimismo, la orden debe contener una declaración de que ésta ha sido emitida en virtud del presente Protocolo. Al hacer esa declaración, la Parte atestigua que la orden se ajusta a los términos del presente Protocolo.

103. En cuanto a la diferencia entre el párrafo 3.a (la autoridad emisora) y el párrafo 3.e (la autoridad que solicita la información relativa al abonado), en algunas Partes, la autoridad emisora y la autoridad que solicita los datos no son las mismas. Por ejemplo, las autoridades que solicitan los datos pueden ser los investigadores o los fiscales, mientras que la orden es dictada por un juez. En tales situaciones, deberá indicarse la autoridad que solicita los datos así como la que emite la orden.

104. No se requiere declaración de los hechos, teniendo en cuenta que esa información es confidencial en la mayoría de las investigaciones penales y no puede ser divulgada a una parte privada.

Párrafo 4

105. Mientras que el párrafo 3 establece la información mínima requerida para las órdenes emitidas en virtud del párrafo 1, ocurre frecuentemente que esas órdenes pueden ejecutarse sólo si el proveedor del servicio (y, en su caso, la autoridad designada por la Parte receptora en virtud del párrafo 5) recibe información complementaria. Por lo tanto, el párrafo 4 del artículo 7 especifica que la autoridad emisora deberá: aportar información complementaria sobre los fundamentos jurídicos internos que facultan a la autoridad para emitir la orden; indicar referencia a las disposiciones legales y a las sanciones aplicables al delito objeto de investigación o enjuiciamiento; incluir información de contacto de la autoridad a la que el proveedor de servicios deberá devolver la información relativa al abonado, solicitar más información o responder de otro modo; determinar el plazo y la forma de devolver la información relativa al abonado; exponer si ya se ha solicitado la conservación de los datos, incluida la fecha de conservación y cualquier número de referencia aplicable; señalar toda instrucción procesal especial (por ejemplo, solicitudes de confidencialidad o autenticación), incluir una declaración, si fuera aplicable, que indique que se ha hecho una notificación simultánea en virtud del párrafo 5, y proveer cualquier información adicional que pueda ayudar a obtener la divulgación de la información relativa al abonado. En la información de contacto no es necesario indicar una persona determinada, sino sólo su función. Esa información complementaria puede facilitarse por separado, pero también puede incluirse en la orden, si así lo permite la legislación de la Parte emisora. Tanto la orden como la información complementaria se transmitirán directamente al proveedor de servicios.

106. Las instrucciones procesales especiales incluyen, en particular, toda solicitud de confidencialidad, incluida la solicitud de no divulgación de la orden al abonado o a terceros, con la salvedad de que las instrucciones procesales especiales no podrán impedir que el proveedor consulte a las autoridades que deben ser notificadas con arreglo al párrafo 5.a, o consultadas de conformidad con el párrafo 5.b. Si se requiere confidencialidad para evitar una divulgación prematura del contenido, ello deberá indicarse en la solicitud. En algunas Partes, la confidencialidad de la orden se mantendrá por imperativo legal, mientras que en otras Partes no es necesariamente así. Por lo tanto, para evitar el riesgo de divulgación prematura de la investigación, se alienta a las Partes

a que tengan en cuenta la legislación aplicable y las políticas del proveedor de servicios relativas a la notificación al abonado antes de presentar la orden en virtud del párrafo 1 al proveedor de servicios. Asimismo, las instrucciones procesales especiales podrán incluir la especificación del canal de transmisión que mejor se adapte a las necesidades de la autoridad. El proveedor de servicios también podrá solicitar información adicional sobre la cuenta u otra información que le ayude a dar una respuesta rápida y completa. Una solicitud de confidencialidad no deberá impedir que los proveedores de servicios informen de manera transparente acerca de las cifras agregadas anónimas de las órdenes recibidas en virtud del artículo 7.

Párrafo 5

107. De conformidad con el párrafo 5.a, una Parte podrá notificar al Secretario General del Consejo de Europa que, cuando se emita una orden en virtud del párrafo 1 a un proveedor de servicios en su territorio, dicha Parte exigirá notificación simultánea, en todos los casos (es decir, para todas las órdenes transmitidas a los proveedores de servicios en su territorio), o bien en circunstancias determinadas.

108. De acuerdo con el párrafo 5.b, una Parte también podrá, con arreglo a su legislación nacional, exigir a un proveedor de servicios que haya recibido una orden de otra Parte que consulte con ella en circunstancias determinadas. Una Parte no podrá exigir consultas para todas las órdenes, lo que añadiría un paso adicional que podría retrasar significativamente la tramitación de las solicitudes, sino sólo en circunstancias más restringidas y determinadas. Los requisitos en materia de consultas deben limitarse a las circunstancias en las que sea más probable que pudiera ser necesario imponer una condición o invocar un motivo de denegación, o en que exista una preocupación acerca del posible perjuicio para las investigaciones o los procedimientos penales de la Parte que transfiere.

109. Los procedimientos de notificación y de consulta son totalmente discrecionales. Una Parte no está obligada a exigir ninguno de los dos procedimientos.

110. Las Partes notificadas en virtud del párrafo 5.a, o consultadas en virtud del párrafo 5.b, podrán ordenar a un proveedor de servicios que no divulgue información por los motivos previstos en el párrafo 5.c, que se exponen con mayor detalle en el párrafo 141 del Informe explicativo sobre el artículo 8. Debido a ello, la posibilidad de que una Parte sea notificada o consultada supone una salvaguardia adicional. Ahora bien, la cooperación debe ser, en principio, amplia, y los impedimentos deben estar estrictamente limitados.

En consecuencia, como se explica en los párrafos 242 y 253 del Informe explicativo del Convenio, la determinación por la Parte notificada o consultada de las condiciones y denegaciones que serían aplicables en virtud del artículo 25, párrafo 4, y del artículo 27, párrafo 4, del Convenio también debería limitarse en consonancia con los objetivos del artículo 7 del Protocolo a fin de eliminar los obstáculos y contemplar procedimientos más eficientes y acelerados para el acceso transfronterizo a pruebas electrónicas para las investigaciones penales.

111. De conformidad con el párrafo 5.d, las Partes que formulen una declaración en virtud del párrafo 5.a, o que requieran consulta en virtud del párrafo 5.b, podrán ponerse en contacto con la autoridad emisora designada con arreglo al párrafo 4.c, y solicitarle información adicional, a fin de determinar si existe fundamento en virtud del párrafo 5.c para ordenar al proveedor de servicios que no cumpla la orden. Se aspira a que el proceso sea tan rápido como lo permitan las circunstancias. La Parte notificada o consultada debe reunir la información necesaria y tomar su decisión en virtud del párrafo 5.c "sin demora injustificada". Cuando sea necesario, para permitir la cooperación, el procedimiento previsto en el párrafo 5.d también puede ofrecer una oportunidad para aclarar aspectos de la confidencialidad de la información solicitada, así como cualquier restricción de la utilización prevista por la autoridad que solicita los datos. Asimismo, esa Parte deberá notificar sin demora a la autoridad de la Parte emisora en caso de que decida dar instrucciones al proveedor de servicios para que no cumpla, así como indicar las razones para hacerlo.

112. La Parte que exija notificación o consulta podrá decidir imponer al proveedor un plazo de espera antes de que éste facilite la información relativa al abonado en respuesta a la orden, con el fin de permitir la notificación o consulta y cualquier solicitud de información adicional que pueda presentar la Parte.

113. De conformidad con el párrafo 5.e, una Parte que requiera notificación o consulta deberá designar una única autoridad y, cuando se requiera notificación en virtud del párrafo 5.a, proporcionar al Secretario General del Consejo de Europa la información de contacto pertinente.

114. Una Parte podrá modificar su obligación de notificación o de consulta en todo momento, dependiendo de su determinación de cualquier factor que sea relevante para ello como, por ejemplo, su deseo de pasar de un régimen de notificación a un régimen de consulta; también podrá hacerlo de estar suficientemente satisfecha con la cooperación directa como para poder revisar o eliminar un requisito anterior de notificación o consulta. Asimismo, puede

decidir que, como resultado de la experiencia adquirida con el mecanismo de cooperación directa, desea instituir un régimen de notificación o consulta.

115. En virtud del párrafo 5.f, el Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de todos los requisitos de notificación de las Partes previstos en los párrafos 5.a y 5.e. La existencia de un registro público y actualizado es fundamental para garantizar que las autoridades y los proveedores de servicios de la Parte emisora estén informados de los requisitos de notificación de cada Parte, que, como ya se ha señalado, pueden cambiar en cualquier momento. Dado que cada Parte puede efectuar dicho cambio a su discreción, cada Parte que haga cualquier cambio o detecte cualquier inexactitud en el registro deberá inmediatamente ponerlo en conocimiento del Secretario General a fin de garantizar que los demás estén informados de los requisitos vigentes actuales y puedan aplicarlos debidamente.

Párrafo 6

116. El párrafo 6 aclara que está permitido presentar una notificación, así como información adicional, a otra Parte en formato electrónico, incluido el uso del correo electrónico y los portales electrónicos. Si fuera aceptable para el proveedor de servicios, una Parte podrá presentar en formato electrónico una orden en virtud del párrafo 1 y la información complementaria en virtud del párrafo 4. La finalidad es fomentar el empleo de medios electrónicos si fueran aceptables para el proveedor de servicios, ya que estos son casi siempre los medios de comunicación más eficientes y rápidos. Los métodos de autenticación podrán incluir diversos medios, o una combinación de medios, que permitan una identificación segura de la autoridad requirente. Esos medios pueden incluir, por ejemplo, la obtención de confirmación de la autenticidad a través de una autoridad conocida de la Parte emisora (por ejemplo, del remitente o de una autoridad central o designada); comunicaciones posteriores entre la autoridad emisora y la Parte receptora; el uso de una dirección de correo electrónico oficial, o futuros métodos de verificación tecnológica que puedan ser utilizados fácilmente por las autoridades emisoras. Un texto similar figura en el párrafo 2 del artículo 10, y en el párrafo 174 del Informe explicativo se proporciona orientación adicional con respecto al requisito en materia de seguridad. El artículo 6, párrafo 4, y el artículo 8, párrafo 5 del Protocolo también contienen un texto similar.

Párrafo 7

117. El párrafo 7 dispone que, si un proveedor de servicios no cumple una orden emitida en virtud del artículo 7, la Parte emisora podrá solicitar la

ejecución solamente en virtud del artículo 8 u otra forma de asistencia mutua. Las Partes que actúen de conformidad con el presente artículo no podrán solicitar la ejecución unilateral.

118. Para la ejecución de la orden en virtud del artículo 8, el presente Protocolo contempla un procedimiento simplificado para la conversión de una orden emitida en virtud de este artículo en una orden en virtud del artículo 8 a fin de aumentar las posibilidades de la Parte emisora para obtener información relativa al abonado.

119. Para evitar la duplicación de esfuerzos, la Parte emisora deberá conceder al proveedor de servicios 30 días o el plazo estipulado en el párrafo 4.d, si este fuera más largo, para llevar a cabo el proceso de notificación y consulta y para que el proveedor de servicios divulgue la información o indique su negativa a hacerlo. Sólo después de transcurrido ese plazo, o si antes de que haya expirado ese plazo el proveedor ha indicado su rechazo a cumplir la orden, la Parte emisora podrá solicitar la ejecución con arreglo al artículo 8 o recurrir a otras formas de asistencia mutua. Con el fin de que las autoridades puedan evaluar si deben solicitar la ejecución en virtud del párrafo 7, se anima a los proveedores de servicios a que expliquen las razones por las que no facilitan los datos solicitados. Por ejemplo, un proveedor de servicios podría explicar que los datos ya no están disponibles.

120. Si una autoridad notificada en virtud del párrafo 5.a, o consultada en virtud del párrafo 5.b, hubiere informado a la Parte emisora de que el proveedor de servicios ha recibido instrucciones de no revelar la información solicitada, la Parte emisora podrá, no obstante, solicitar la ejecución de la orden con arreglo al artículo 8 u otra forma de asistencia mutua. Sin embargo, se corre el riesgo de que esa nueva solicitud sea también denegada. Se recomienda a la Parte emisora que realice consultas previas con una autoridad designada en virtud de los párrafos 5.a o 5.b para subsanar cualquier deficiencia en la orden original y evitar el rechazo de órdenes presentadas en virtud del artículo 8, o a través de cualquier otro mecanismo de asistencia mutua.

Párrafo 8

121. De conformidad con el párrafo 8, una Parte podrá formular una declaración en la que estipule que otra Parte deberá solicitar al proveedor de servicios la divulgación de la información relativa a los abonados antes de solicitarla en virtud del artículo 8, a menos que la Parte emisora diere una explicación razonable de por qué no lo ha hecho. Por ejemplo, una Parte puede hacer tal declaración porque considera que los procedimientos previstos en el presente artículo deberían permitir a otras Partes obtener los datos relativos a los

abonados más rápido de lo previsto en el artículo 8 y, en consecuencia, podría reducir el número de situaciones en las que es necesario invocar el artículo 8. En ese caso, se recurriría a los procedimientos del artículo 8 solamente cuando resultaren infructuosos los esfuerzos para obtener directamente del proveedor de servicios la información relativa al abonado, cuando la Parte emisora tuviera una explicación razonable para no invocar primero este artículo, o cuando la Parte emisora se hubiera reservado el derecho de no aplicar el presente artículo. Por ejemplo, como demostración, una Parte emisora podrá aducir que un proveedor de servicios habitualmente no proporciona información relativa a los abonados en respuesta a las órdenes recibidas directamente de esa Parte. Otro ejemplo: si una Parte emite solamente una orden en la que solicita tanto información relativa a los abonados como datos sobre el tráfico a otra Parte que aplica el artículo 8 a ambas categorías de datos, la Parte emisora no tendría que solicitar primero por separado la información relativa a los abonados.

Párrafo 9

122. De conformidad con el párrafo 9.a, una Parte que se reserve el derecho de no aplicar este artículo no está obligada a adoptar medidas en virtud del párrafo 2 para que los proveedores de servicios en su territorio divulguen información relativa a los abonados en respuesta a órdenes emitidas por otras Partes. Una Parte que se reserve el derecho de no aplicar este artículo no está autorizada a emitir órdenes en virtud del párrafo 1 a los proveedores de servicios en los territorios de otras Partes.

123. El párrafo 9.b dispone que - por las razones explicadas en el párrafo 93 *supra* - si la divulgación de determinados tipos de números de acceso con arreglo a este artículo fuera incompatible con los principios fundamentales de su ordenamiento jurídico interno, una Parte podrá reservarse el derecho de no aplicar este artículo a esos números. Una Parte que se reserve ese derecho no está autorizada a emitir órdenes relativas a tales números en virtud del párrafo 1 a proveedores de servicios en los territorios de otras Partes.

Sección 3 - Procedimientos para mejorar la cooperación internacional entre autoridades para la divulgación de datos informáticos almacenados

Artículo 8 - Dar efecto a las órdenes de otra Parte para la producción acelerada de información relativa a los abonados y datos sobre el tráfico

124. La finalidad del artículo 8 es que la Parte requirente tenga la capacidad de emitir una orden que se presentará a otra Parte en el marco de una solicitud, y

que la Parte requerida tenga la capacidad de dar efecto a esa orden con el fin de obligar a un proveedor de servicios en su territorio a presentar información relativa a los abonados o datos sobre el tráfico en posesión o bajo el control del proveedor de servicios.

125. Este artículo establece un mecanismo que complementa las disposiciones en materia de asistencia mutua del Convenio. Está concebido para ser más ágil que la asistencia mutua existente, en la medida en que la información que debe facilitar la Parte requirente es más limitada, y que el proceso para obtener los datos es más rápido. Este artículo sirve de complemento, y por lo tanto se entiende sin perjuicio de otros procesos de asistencia mutua en el marco del Convenio, o de otros acuerdos multilaterales o bilaterales, que una Parte sigue siendo libre de invocar. De hecho, en situaciones en las que una Parte requirente solicite datos sobre el tráfico a una Parte que haya formulado una reserva a ese aspecto del artículo 8, la Parte requirente podrá recurrir a otro procedimiento de asistencia mutua. Cuando, como suele ser el caso, se solicita simultáneamente información relativa al abonado, datos sobre el tráfico y datos sobre el contenido almacenados, podría ser más eficiente pedir los tres tipos de datos para la misma cuenta englobándolos en una única solicitud de asistencia mutua tradicional, en lugar de tratar de obtener algunos tipos de datos por el método previsto en este artículo y otro tipo de información mediante una solicitud de asistencia mutua enviada por separado.

Párrafo 1

126. El párrafo 1 dispone que la Parte requirente podrá emitir una orden en que recabe información relativa a los abonados o datos sobre el tráfico de un proveedor de servicios en el territorio de otra Parte. En el artículo 8, por "orden" se entiende cualquier proceso legal que tiene por objeto obligar a un proveedor de servicios a entregar información relativa a los abonados o datos sobre el tráfico. Por ejemplo, se puede instrumentar mediante una orden de presentación, una citación u otro mecanismo autorizado por la ley y que pueda emitirse con el fin de imponer la divulgación de información relativa a los abonados o datos sobre el tráfico.

127. Tal y como se define en el párrafo 2.b. del artículo 3, la "autoridad competente" en el párrafo 1 del presente artículo se refiere a una "autoridad judicial, administrativa u otra autoridad encargada de hacer cumplir la ley que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas en virtud del presente Protocolo con el fin de obtener o presentar pruebas en relación con investigaciones o procedimientos penales

específicos". Cabe señalar que las autoridades competentes para dictar una orden en virtud del párrafo 1 pueden no ser necesariamente las mismas que las autoridades designadas para presentar la orden a la que se dará efecto de conformidad con el párrafo 10.a del artículo 8, como se describe en mayor detalle a continuación.

128. En el artículo 8, el término "un proveedor de servicios en el territorio de la Parte requerida" exige la presencia física del proveedor de servicios en la otra Parte. En virtud de este artículo, el mero hecho de que, por ejemplo, un proveedor de servicios haya establecido una relación contractual con una empresa de una Parte, pero el propio proveedor de servicios no esté físicamente presente en esa Parte, no quiere decir que el proveedor de servicios se encuentra "en el territorio" de esa Parte. El párrafo 1 requiere, además, que los datos estén en posesión o control del proveedor de servicios.

Párrafo 2

129. En virtud del párrafo 2, la Parte requerida adoptará las medidas necesarias para dar efecto en su territorio a una orden emitida en virtud del párrafo 1, con sujeción a las salvaguardias que se describen más adelante. "Dar efecto" significa que la Parte requerida obligará al proveedor de servicios a facilitar información relativa a los abonados y datos sobre el tráfico empleando el mecanismo que elija la Parte requerida, siempre que dicho mecanismo permita que la orden sea ejecutable con arreglo a la legislación nacional de la Parte requerida y cumpla los requisitos del presente artículo. Por ejemplo, una Parte requerida podrá dar efecto a la orden de una Parte requirente aceptándola como equivalente a las órdenes nacionales, refrendándola para que surta el mismo efecto que una orden nacional, o emitiendo su propia orden de presentación. Cualquier mecanismo de este tipo estará sujeto a los términos de la legislación de la Parte requerida, ya que estará regido por los procedimientos de la Parte requerida. Por lo tanto, la Parte requerida puede garantizar el cumplimiento de lo dispuesto en su propia legislación, incluidos los requisitos constitucionales y en materia de derechos humanos, especialmente en relación con cualquier salvaguardia adicional, incluidas las necesarias para la presentación de datos sobre el tráfico.

130. Si bien este artículo puede cumplimentarse de varias maneras, una Parte tal vez desee estructurar sus propios procesos internos dotándolos de la flexibilidad necesaria para dar cuenta de las solicitudes de diversas autoridades competentes. El párrafo 3.b se negoció para garantizar que la Parte requerida reciba información suficiente para garantizar que pueda

llevar a cabo un examen completo en caso necesario, ya que algunas Partes indicaron que emitirían su propia orden para dar efecto a la orden de la Parte requirente.

Párrafo 3

131. Para poner en marcha el proceso de la Parte requerida para dar efecto a la orden, la Parte requirente transmitirá la orden y la información de apoyo. El párrafo 3 precisa los elementos que la Parte requirente debe facilitar a la Parte requerida para que ésta pueda dar efecto a la orden y obligar al proveedor de servicios en su territorio a entregar la información. El párrafo 3.a especifica la información que debe figurar en la orden, e incluye información que es fundamental para su ejecución. La información especificada en el párrafo 3.b, que es para uso exclusivo de la Parte requerida y no se dará a conocer al proveedor de servicios sin el consentimiento de la Parte requirente, es información de apoyo que establece los fundamentos jurídicos nacionales e internacionales para la orden en el presente Protocolo, e incluye información que permite a la Parte requerida evaluar los posibles motivos para poner condiciones o denegar la entrega con arreglo al párrafo 8. Al dar inicio a una solicitud en virtud del artículo 8, las Partes deberán indicar si disponen de información con arreglo al párrafo 3.b que pueda ser compartida con el proveedor de servicios. De conformidad con el párrafo 3.c, la solicitud también deberá incluir todas las instrucciones procesales especiales, incluidas, por ejemplo, las solicitudes de certificación o confidencialidad de la solicitud (análogo al artículo 27, párrafo 8, del Convenio, en el momento de la transmisión a fin de garantizar la correcta tramitación de la solicitud.

132. La orden para obtener información relativa a los abonados o datos sobre el tráfico descrita en el párrafo 3.a deberá especificar en su anverso: i) la autoridad que emitió la orden y la fecha en que fue emitida; ii) una declaración de que se expide en virtud del presente Protocolo; iii) el nombre y dirección del proveedor o proveedores de servicios que serán notificados; iv) el delito objeto de la investigación o del procedimiento penal; v) la autoridad que recaba los datos, si no fuera la autoridad emisora, y vi) una descripción detallada de los datos concretos solicitados (es decir, la identidad del abonado, su dirección postal o geográfica, su número de teléfono u otro número de acceso), y la información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios (véase el artículo 3 del presente Protocolo en que se incorpora el artículo 18, párrafo 3 del Convenio y el párrafo 93 *supra* del Informe explicativo); y, en relación con los datos sobre el tráfico, indicar los datos informáticos relativos a una

comunicación por medio de un sistema informático, generados por un sistema informático que formó parte de la cadena de comunicación que precisen el origen, el destino, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente de la comunicación (véase el artículo 3, párrafo 1 del presente Protocolo, en que se incorpora el artículo 3, párrafo 1, del presente Protocolo que incorpora el artículo 1, párrafo d. del Convenio). Con respecto al párrafo 3.a.v, si la autoridad que emite la orden no fuera la misma que la que pide los datos, la disposición exige la identificación de ambas. Por ejemplo, los datos pueden ser solicitados por una autoridad investigadora o fiscal, mientras que la orden puede ser emitida por un juez. Esta información demuestra la legitimidad de la orden y estipula instrucciones claras para su ejecución.

133. La información de apoyo especificada en el párrafo 3.b tiene por objeto proporcionar a la Parte requerida la información que necesitaría para dar efecto a la orden recibida de la Parte requirente. Para facilitar el procedimiento se podría adoptar también una plantilla fácil de rellenar, lo que permitiría aumentar la eficiencia del proceso. En la lista de información de apoyo se incluye lo siguiente:

a. El párrafo 3.b.i se refiere a los fundamentos jurídicos internos que facultan a la autoridad emisora para emitir la orden de presentación. En otras palabras, ésta es la legislación pertinente que faculta a una autoridad competente para emitir la orden descrita en el párrafo 1.

b. El párrafo 3.b.ii se refiere a las disposiciones legales relativas al delito a que se hace referencia en la orden en el párrafo 3.a.iv y las sanciones aplicables. La inclusión de ambos elementos es importante para que la Parte requerida pueda evaluar si la solicitud está o no dentro del ámbito de sus obligaciones.

c. El párrafo 3.b.iii se refiere a toda información que la Parte requirente pueda suministrar que le haya llevado a concluir que el proveedor o proveedores de servicios objeto de la orden están en posesión o control de la información o los datos solicitados. Esa información es fundamental para dar inicio al proceso en la Parte requerida. La identificación del proveedor de servicios nacional y la convicción de que posee o controla la información o los datos recabados suele ser un requisito previo para dar inicio a las solicitudes de órdenes de presentación.

d. El párrafo 3.b.iv se refiere a un breve resumen de los hechos relacionados con la investigación o el procedimiento. Esta información también es un factor esencial para que la Parte requerida pueda determinar si una orden en virtud de este artículo debe surtir efecto en su territorio;

e. El párrafo 3.b.v se refiere a una declaración sobre la relevancia de la información o los datos para la investigación o el procedimiento. Esa declaración está destinada a ayudar a la Parte requerida a decidir si se cumplen o no los requisitos del párrafo 1 del presente artículo, es decir, que la información o los datos son "necesarios para las investigaciones o los procedimientos penales específicos de la Parte-

f. El párrafo 3.b.vi se refiere a la información de contacto de una autoridad o autoridades en caso de que la autoridad competente de la Parte requerida precise información adicional para dar efecto a la orden;

g. El párrafo 3.b.vii se refiere a la información sobre si ya se ha solicitado la conservación de la información o los datos. Esta información es importante para la Parte requerida, especialmente en relación con los datos sobre el tráfico, y deberá incluir, por ejemplo, los números de referencia y la fecha de conservación ya que esa información puede permitir a la Parte requerida cotejar la solicitud actual con una solicitud de conservación anterior y, por tanto, facilitar la divulgación de la información o los datos conservados originalmente. Para reducir el riesgo de supresión de la información o los datos, se insta a las Partes a que procuren preservar la información o los datos solicitados lo antes posible y a que, antes de presentar una solicitud en virtud de este artículo, y procuren que la conservación se prolongue oportunamente;

h. El párrafo 3.b.viii se refiere a información sobre si ya se ha tratado de obtener los datos por otros medios y, si así fuera, de qué manera. Esta disposición se refiere principalmente a la posibilidad de que la Parte requirente ya hubiera solicitado información relativa al abonado o datos sobre el tráfico directamente del proveedor de servicios.

134. La información que debe facilitarse de conformidad con el párrafo 3.b no se dará a conocer al proveedor de servicios sin el consentimiento de la Parte requirente. En particular, el resumen de los hechos y la declaración relativa a la pertinencia de la información o los datos para la investigación o el procedimiento se facilitan a la Parte requerida a fin de que ésta pueda determinar si existe un motivo para imponer términos o condiciones, o para rechazar la solicitud, pero suelen estar sujetos al secreto de la investigación.

135. En virtud del párrafo 3.c, la Parte requirente podrá solicitar que la Parte requerida aplique instrucciones procesales especiales, incluidas las solicitudes de no divulgación de la orden al abonado o los formularios de autenticación de las pruebas que deben rellenarse. Esa información deberá

conocerse desde un inicio, ya que las instrucciones especiales pueden conllevar procesos adicionales en la Parte requerida.

136. Para dar efecto a la orden y facilitar aún más la presentación de la información o los datos, la Parte requerida podrá facilitar al proveedor de servicios información adicional, como el método de presentación y la autoridad a la que deben presentar los datos en la Parte requerida.

Párrafo 4

137. De conformidad con el párrafo 4, puede ser necesario ofrecer información adicional a la Parte requerida para que ésta pueda dar efecto a la orden. Por ejemplo, en virtud de la legislación interna de algunas Partes, la presentación de datos sobre el tráfico puede exigir información adicional ya que en su legislación existen requisitos adicionales en relación con la obtención de dichos datos. Así mismo, la Parte requerida puede pedir aclaraciones sobre la información proporcionada de conformidad con el párrafo 3.b. Como nuevo ejemplo, algunas Partes pueden exigir información adicional cuando la orden no haya sido emitida o verificada por un fiscal u otra autoridad judicial o administrativa independiente de la Parte requirente. Al formular tal declaración, las Partes deberán ser lo más específicas posible con respecto al tipo de información adicional necesaria.

Párrafo 5

138. En virtud del párrafo 5, la Parte requerida aceptará solicitudes en formato electrónico. Podrá exigir el empleo de medios adecuados de seguridad y autenticación de las comunicaciones electrónicas para facilitar la transmisión de información, datos y documentos, incluida la transmisión de órdenes y la información de apoyo. Esos medios de comunicación están previstos también en los artículos 6 al 11.

Párrafo 6

139. De conformidad con el párrafo 6, la Parte requerida adoptará medidas razonables para tramitar rápidamente la solicitud. Hará esfuerzos razonables para tramitar las solicitudes y notificar al proveedor de servicios en un plazo de cuarenta y cinco días después de que la Parte requerida haya recibido todos los documentos e información necesarios. La Parte requerida ordenará al proveedor de servicios que devuelva la información relativa al abonado en un plazo de veinte días y los datos sobre el tráfico en un plazo de cuarenta y cinco días. Si bien la Parte requerida debe tratar de lograr la presentación de la información lo más rápidamente posible, hay muchos factores que pueden

retrasarla, como la objeción de los proveedores de servicios; la falta de respuesta a las solicitudes; el incumplimiento del plazo de entrega de la información, y el volumen de solicitudes que tenga que tramitar una Parte requerida. Debido a ello, se ha decidido exigir a las Partes requeridas que hagan esfuerzos razonables para completar únicamente los procesos que estén bajo su control.

Párrafo 7

140. Las Partes reconocieron que algunas instrucciones procesales especiales de la Parte requirente también pueden causar retrasos en la tramitación de las órdenes, si las instrucciones requieren procesos internos adicionales para dar efecto a esas instrucciones. Asimismo, la Parte requerida podrá exigir de la Parte requirente información adicional para respaldar cualquier solicitud de órdenes complementarias, como las órdenes de confidencialidad (órdenes de no divulgación). Es posible que algunas instrucciones procesales no estén acordes con la legislación de la Parte requerida, en cuyo caso el párrafo 7 dispone que ésta informará sin demora a la Parte requirente y especificará las condiciones en las que podría acceder, tras lo cual la Parte requirente determinará si, a pesar de todo, la solicitud debe ser ejecutada.

Párrafo 8

141. En virtud del párrafo 8, la Parte requerida podrá negarse a ejecutar una solicitud atendiendo a los motivos de denegación establecidos en el artículo 25, párrafo 4, o en el artículo 27, párrafo 4 del Convenio. Por ejemplo, en consonancia con el párrafo 257 del Informe explicativo del Convenio, esta disposición está sujeta a los motivos de denegación previstos en los tratados de asistencia mutua aplicables y en el derecho interno y establece "salvaguardias para los derechos de las personas que se encuentran en el territorio de la Parte requerida", y, en consonancia con el párrafo 268 de dicho Informe explicativo, la asistencia podrá denegarse por motivos de "perjuicio a la soberanía del Estado, a la seguridad, al orden público o a otros intereses fundamentales". También podrá imponer condiciones que son necesarias para permitir la ejecución de la solicitud, como la confidencialidad. Asimismo, la Parte requerida podrá aplazar la ejecución de la solicitud en virtud del artículo 27, párrafo 5, del Convenio. La Parte requerida notificará a la Parte requirente su decisión de denegar, condicionar o aplazar la solicitud. Además, las Partes podrán aplicar la restricción de utilización con arreglo a los términos del artículo 28, párrafo 2.b del Convenio.

142. Con el fin de potenciar el principio de estimular la cooperación en la mayor medida posible (véase el artículo 5, párrafo 1), los motivos de denegación

establecidos por una Parte requerida deberán ser limitados y ejercidos con moderación. Cabe recordar que el párrafo 253 del Informe explicativo del Convenio establece que "la asistencia mutua ha de ser, en principio, amplia, y los obstáculos a la misma deberán estar estrictamente limitados". En consecuencia, las condiciones y los rechazos también deben limitarse acorde con los objetivos de este artículo a fin de eliminar los obstáculos al intercambio transfronterizo de la información relativa a los abonados y los datos sobre el tráfico y de establecer procedimientos más rápidos y eficaces que la asistencia mutua tradicional.

Párrafo 9

143. De conformidad con el párrafo 9, "[s]i la Parte requirente no puede cumplir una condición impuesta por la Parte requerida en virtud del párrafo 8, informará sin demora a la Parte requerida. La Parte requerida determinará entonces si, a pesar de ello, debe facilitarse la información o el material. Si la Parte requirente acepta la condición, quedará obligada a cumplirla. La Parte requerida que suministre información o material sujeto a dicha condición podrá exigir a la Parte requirente que explique, en relación con dicha condición, el uso que se ha hecho de dicha información o material."

Párrafo 10

144. La finalidad del párrafo 10 es garantizar que las Partes, en el momento de la firma, o al depositar sus instrumentos de ratificación, aceptación o aprobación, indiquen cuáles serán las autoridades que presentarán y recibirán órdenes en virtud del artículo 8. Las Partes no tendrán que dar el nombre y la dirección de una persona concreta, sino que podrán indicar un cargo o dependencia que se haya considerado competente para los fines del envío y recepción de órdenes con arreglo al presente artículo.

Párrafo 11

145. El párrafo 11 permite a una Parte formular una declaración en que exija que las órdenes presentadas en virtud de este artículo sean transmitidas por la autoridad central de la Parte requirente, u otra autoridad, cuando así lo hayan determinado las Partes. Se alienta a las Partes a que brinden la mayor flexibilidad posible en cuanto a la presentación de solicitudes.

Párrafo 12

146. El párrafo 12 dispone que el Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de las autoridades designadas

por las Partes según lo dispuesto en el párrafo 10; cada Parte deberá velar por que los datos que figuran en el registro sean correctos. Esa información ayudará a las Partes requeridas a verificar la autenticidad de las solicitudes.

Párrafo 13

147. De conformidad con el párrafo 13, una Parte que se reserve el derecho de no aplicar este artículo a los datos sobre el tráfico no está obligada a dar curso a las órdenes en que se recaben datos sobre el tráfico emitidas por otra Parte. Una Parte que se reserve este derecho no está autorizada a presentar a otras Partes órdenes para obtener datos sobre el tráfico en virtud del párrafo 1.

Artículo 9 - Divulgación acelerada de datos informáticos almacenados en caso de emergencia

148. Además de las demás formas de cooperación acelerada previstas en el presente Protocolo, quienes participaron en la redacción eran conscientes de la necesidad de potenciar la capacidad de las Partes, en caso de emergencia, para obtener rápidamente datos informáticos específicos almacenados en posesión o bajo el control de un proveedor de servicios en el territorio de otra Parte para su utilización en investigaciones o procedimientos penales específicos. Como se expone en los párrafos 42 y 172 del presente Informe explicativo, la necesidad de una cooperación máxima acelerada puede presentarse en distintas situaciones urgentes, como en el período inmediatamente posterior a un ataque terrorista, en el caso de un ataque de *ransomware* que pueda paralizar el sistema de un hospital, o cuando se investigan las cuentas de correo electrónico utilizadas por los secuestradores para enviar demandas y comunicarse con la familia de la víctima.

149. En virtud del Convenio, en caso de emergencia, las Partes formulan solicitudes de asistencia mutua para obtener datos y, en virtud del artículo 35, párrafo 1.c del Convenio, la Red 24/7 está disponible para facilitar la ejecución de esas solicitudes. Por otra parte, los ordenamientos jurídicos de algunos países permiten a las autoridades competentes de otros países solicitar la divulgación de datos con carácter urgente a través de la Red 24/7 sin que sea necesario enviar una solicitud de asistencia mutua.

150. Como se refleja en el artículo 5, párrafo 7, este artículo no prejuzga la cooperación (incluida la cooperación espontánea) entre las Partes, o entre las Partes y los proveedores de servicios, a través de otros acuerdos, convenios, prácticas o leyes nacionales aplicables. Por consiguiente, en virtud del presente Protocolo, todos los mecanismos mencionados siguen estando a disposición

de las autoridades competentes que recaban datos en caso de emergencia. La innovación de este Protocolo es la elaboración de dos artículos que obligan a todas las Partes a establecer, como mínimo, canales específicos para una cooperación rápida y expedita en situaciones de emergencia: el artículo 9 y el artículo 10.

151. Este artículo permite a las Partes cooperar para obtener datos informáticos en caso de emergencia canalizando sus solicitudes a través de la Red 24/7 establecida por el artículo 35 del Convenio. La Red 24/7 es adecuada sobre todo para dar cuenta de las solicitudes urgentes y de gran prioridad previstas en este artículo. La Red cuenta con puntos de contacto que, en la práctica, se comunican rápidamente y sin necesidad de traducciones escritas y están en condiciones de atender las solicitudes recibidas de otras Partes, ya sea dirigiéndose directamente a los proveedores en su territorio, solicitando la asistencia de otras autoridades competentes o recurriendo a las autoridades judiciales, si así lo exige el derecho interno de la Parte. Los puntos de contacto también pueden asesorar a las Partes requirentes sobre las cuestiones que pudieran tener en relación con los proveedores y la obtención de pruebas electrónicas, por ejemplo, explicando la legislación interna que se debe acatar para la obtención de pruebas. Esa comunicación en doble sentido mejora la comprensión por la Parte requirente de la legislación interna de la Parte requerida y facilita la obtención más fluida de las pruebas necesarias.

152. El uso del canal establecido en el presente artículo puede tener ventajas con respecto al canal de asistencia mutua en caso de emergencia establecido en el artículo 10. Por ejemplo, este canal tiene la ventaja de que no es necesario preparar con antelación ninguna solicitud de asistencia mutua. Puede ser necesario un tiempo considerable para preparar una solicitud previa de asistencia mutua, traducirla y transmitirla por los canales nacionales a la autoridad central de asistencia recíproca de la Parte requirente, lo que no sería necesario en virtud del artículo 9. Además, una vez que la Parte requerida ha recibido la solicitud, si necesitara obtener información complementaria antes de poder conceder la asistencia, es muy probable que el tiempo adicional que fuera necesario para la presentación de una solicitud de asistencia mutua retrasase la ejecución de la solicitud. En el contexto de la asistencia mutua, las Partes a las que se solicita asistencia suelen exigir que la información complementaria se presente por escrito y de forma más detallada, mientras que el canal 24/7 funciona mediante el intercambio de información en tiempo real. Por otra parte, el canal de asistencia mutua en caso de emergencia ofrece ventajas en determinadas situaciones. Por ejemplo: i) se puede perder poco o nada

de tiempo utilizando ese canal si existen relaciones de trabajo especialmente estrechas entre las autoridades centrales correspondientes; ii) la asistencia mutua en caso de emergencia puede destinarse a obtener formas adicionales de cooperación que van más allá de los datos informáticos en poder de los proveedores, y iii) puede ser más fácil autenticar las pruebas obtenidas mediante la asistencia mutua. Corresponde a las Partes, sobre la base de su experiencia acumulada y de las circunstancias jurídicas y fácticas específicas, decidir cuál es el mejor canal a utilizar en un caso concreto.

Párrafo 1

153. En virtud del párrafo 1.a, cada Parte adoptará las medidas necesarias para garantizar que su punto de contacto para la Red 24/7 pueda, en caso de emergencia, transmitir una solicitud al punto de contacto de otra Parte para pedir asistencia inmediata con el fin de obtener la divulgación acelerada de datos informáticos especificados y almacenados en poder de los proveedores en el territorio de esa Parte, y para recibir solicitudes de los puntos de contacto de otras Partes sobre dichos datos en poder de los proveedores en su territorio. Según lo dispuesto en el artículo 2, la solicitud deberá hacerse en el marco de una investigación o procedimiento penal específico.

154. Los puntos de contacto de la Red 24/7 deben poder transmitir y recibir las solicitudes en caso de emergencia sin que sea necesario preparar y transmitir con antelación una solicitud de asistencia mutua como se describe en el párrafo 152 de este Informe explicativo, sin perjuicio de la posibilidad de hacer una declaración en virtud del artículo 9, párrafo 5. El término "emergencia" se define en el artículo 3. En virtud del artículo 9, la Parte requerida deberá determinar si existe una "emergencia" en relación con una solicitud atendiendo a la información suministrada en el párrafo 3.

155. A diferencia de otros artículos del presente Protocolo, como el artículo 7, que sólo se puede utilizar para obtener "información especificada y almacenada del abonado", este artículo utiliza el término más amplio de "datos informáticos especificados y almacenados". El alcance de este término es amplio pero no indiscriminado: abarca todo dato informático "especificado" con arreglo a la definición del artículo 1.b del Convenio, que ha sido incorporada en el artículo 3, párrafo 1, del presente Protocolo. El empleo de este término más amplio reconoce la importancia de obtener los datos sobre el contenido y sobre el tráfico almacenados, y no sólo la información relativa al abonado, en caso de emergencia sin exigir la presentación previa de una solicitud de asistencia mutua. Los datos en cuestión son datos almacenados o existentes y

no incluyen los datos que aún no existen, como los datos sobre el tráfico o los datos sobre el contenido que guardan relación con comunicaciones futuras (véase el párrafo 170 del Informe explicativo del Convenio).

156. Esta disposición brinda flexibilidad a la Parte requirente para determinar cuál de sus autoridades debe incoar la solicitud, como pueden ser sus autoridades competentes encargadas de la investigación, o su punto de contacto de la Red 24/7, con arreglo a la legislación nacional. El punto de contacto de la Red 24/7 en la Parte requirente pasa a ser entonces el canal para transmitir la solicitud al punto de contacto de la Red 24/7 en la otra Parte.

157. En virtud del párrafo 1.b, una Parte podrá hacer una declaración en la que señale que no dará cumplimiento a aquellas solicitudes emitidas en virtud del artículo 9 que estén destinadas únicamente a obtener información relativa a los abonados, tal como se define en el artículo 18.3 del Convenio, incorporado en el artículo 3, párrafo 1 del presente Protocolo. Para algunas Partes, la recepción de solicitudes emitidas en virtud de este artículo destinadas únicamente a obtener información relativa a los abonados entrañaría el riesgo de sobrecarga de los puntos de contacto de la Red 24/7, al desviar recursos y energía de las solicitudes relativas al contenido o a los datos sobre el tráfico. En tales casos, las Partes que deseen obtener solamente información relativa al abonado podrán invocar los artículos 7 u 8, que facilitan la divulgación rápida de esa información. Dicha declaración no prohíbe a otras Partes incluir una solicitud de información relativa a los abonados cuando emitan también una solicitud sobre el contenido y/o datos sobre el tráfico en virtud del presente artículo.

Párrafo 2

158. Con arreglo al párrafo 2, cada Parte adoptará las medidas necesarias para garantizar que su legislación nacional permita a sus autoridades pedir y obtener datos de un proveedor de servicios en su territorio para dar curso a una solicitud en virtud del párrafo 1 y dar respuesta a tales solicitudes sin que la Parte requirente esté obligada a presentar una solicitud de asistencia mutua, sujeto a la posibilidad de formular una declaración de conformidad con el párrafo 5.

159. En vista de las diferencias entre las legislaciones nacionales, el párrafo 2 tiene como objeto brindar flexibilidad a las Partes en la elaboración de sus sistemas destinados a dar respuesta a solicitudes formuladas en virtud del párrafo 1. No obstante, se alienta a las Partes a elaborar mecanismos para cumplir este artículo que hagan hincapié en la rapidez y eficiencia, que se adapten a las exigencias

de situaciones de emergencia y que brinden una amplia base jurídica para la divulgación de datos a otras Partes en caso de emergencia.

160. Queda a discreción de la Parte requerida determinar: i) si se han cumplido los requisitos para invocar este artículo; ii) si otro mecanismo es adecuado para prestar ayuda a la Parte requirente, y iii) la autoridad competente para ejecutar una solicitud recibida por el punto de contacto de la Red 24/7. Aunque en algunas Partes el punto de contacto de la Red 24/7 puede tener ya la autoridad necesaria para ejecutar la solicitud por sí mismo, otras Partes pueden exigir que el punto de contacto transmita la solicitud a otra u otras autoridades para poder pedir al proveedor que entregue los datos en su poder. En algunas Partes, ello puede exigir la obtención de una orden judicial para pedir la divulgación de los datos. La Parte requerida también goza de poder discrecional para determinar el canal por el que transitarán los datos que se enviarán a la Parte requirente, ya sea a través del punto de contacto 24/7 o por conducto de otra autoridad.

Párrafo 3

161. El párrafo 3 precisa la información que deberá incluirse en una solicitud en virtud del párrafo 1. La información especificada en el párrafo 3 tiene por objeto facilitar el examen y, cuando proceda, la ejecución de la solicitud por parte de la autoridad competente de la Parte requerida.

162. Con respecto al párrafo 3.a, la Parte requirente deberá especificar la autoridad competente en cuyo nombre se solicitan los datos.

163. Con respecto al párrafo 3.b, la Parte requirente deberá indicar que la solicitud se ha emitido en virtud del presente Protocolo. Ello garantizará que la solicitud formulada se atenga a este Protocolo y que cualquier dato recibido como resultado de la misma será tratado de conformidad con lo dispuesto en el presente Protocolo. Este aspecto también diferencia la solicitud de otras solicitudes de divulgación en caso de emergencia que pudiera recibir el punto de contacto de la Red 24/7.

164. Conforme al párrafo 3.e, la Parte requirente deberá aportar hechos suficientes que demuestren la existencia de una emergencia, tal y como se define en el artículo 3, y la forma en que los datos recabados en la solicitud guardan relación con dicha emergencia. En caso de que la Parte requerida pida esclarecimiento de la solicitud o necesite información adicional para dar curso a la solicitud, deberá consultar con el punto de contacto de la Red 24/7 de la Parte requirente.

165. Acorde con el párrafo 3.g, la solicitud deberá especificar cualquier instrucción procesal especial. Éstas incluyen, en particular, la petición de no dar a conocer la solicitud a los abonados o a terceros, ni desvelar los formularios de autenticación que deben rellenarse para los datos solicitados. En virtud de este párrafo, esas instrucciones procesales se presentan desde la etapa inicial, ya que las instrucciones especiales pueden conllevar procesos adicionales en la Parte requerida. En algunas Partes, la confidencialidad puede mantenerse por imperativo legal, mientras que en otras Partes no es necesariamente así. Por lo tanto, con el fin de evitar el riesgo de divulgación prematura de la investigación, se alienta a las Partes a que se comuniquen en cuanto a la necesidad de mantener la confidencialidad y las dificultades que puedan surgir, incluida cualquier ley aplicable, y también acerca de las políticas del proveedor de servicios en lo referente a la notificación. Dado que en muchos casos las solicitudes de autenticación de los datos que forman parte de la respuesta pueden retrasar el objetivo fundamental de la rápida transmisión de los datos solicitados, las autoridades de la Parte requerida, en consulta con las autoridades de la Parte requirente, determinarán el momento y la manera de facilitar la confirmación de su autenticidad.

166. Además, la Parte o el proveedor de servicios podrá exigir información adicional que contribuya a la localización y divulgación de los datos informáticos almacenados solicitados por la Parte requirente.

Párrafo 4

167. El párrafo 4 dispone que la Parte requerida aceptará solicitudes en formato electrónico. Se alienta a las Partes a que utilicen medios de comunicación rápidos para facilitar la transmisión de información o datos y documentos, incluida la transmisión de solicitudes. Este párrafo se basa en el párrafo 5 del artículo 8, pero ha sido modificado para añadir que una Parte puede aceptar solicitudes transmitidas verbalmente, método de comunicación utilizado frecuentemente por la Red 24/7.

Párrafo 5

168. El párrafo 5 permite a una Parte formular una declaración en la que exige a otras Partes que soliciten datos en virtud de este artículo a que, una vez ejecutada la solicitud y transmitidos los datos, la solicitud y toda información complementaria transmitida en apoyo de la misma sea presentada en un formato específico y por un canal específico. Por ejemplo, en su declaración una Parte puede exigir que, en circunstancias concretas, la Parte requirente

presente ulteriormente una solicitud de asistencia mutua a fin de documentar oficialmente la solicitud en caso de emergencia y la decisión previa de facilitar datos en respuesta a dicha solicitud. La legislación interna de algunas Partes exige ese procedimiento; por el contrario, otras Partes han indicado que no tienen tales requisitos y no necesitan hacer una declaración para valerse de esa posibilidad.

Párrafo 6

169. Este artículo se refiere a las "solicitudes" y no exige que las Partes requeridas proporcionen los datos solicitados a las Partes requirentes. Por consiguiente, quienes participaron en la redacción reconocen que habrá situaciones en que las Partes a las que se haya solicitado la información no entregarán los datos pedidos a una Parte requirente en virtud del presente artículo. La Parte requerida podrá determinar que, en un caso concreto, lo más apropiado sería la asistencia mutua en caso de emergencia en virtud del artículo 10, u otro medio de cooperación. En consecuencia, el párrafo 6 dispone que cuando una Parte requerida determinase que no facilitará los datos solicitados a una Parte que hubiere presentado una solicitud con arreglo al párrafo 1 del presente artículo, la Parte requerida informará de su decisión a la Parte requirente de forma rápida y expedita y, si procede, especificará las condiciones en las que podría entregar los datos y explicará cualquier otra forma de cooperación que pudiera estar disponible, con el fin de alcanzar el objetivo mutuo de las Partes de agilizar la divulgación de datos en casos de emergencia.

Párrafo 7

170. El párrafo 7 describe los procedimientos aplicables cuando el Estado requerido haya especificado condiciones para la concesión de la cooperación en virtud del párrafo 6. De conformidad con el párrafo 7a., cuando la Parte requirente no pueda cumplir las condiciones especificadas, deberá ponerlo rápidamente en conocimiento de la Parte requerida y ésta determinará si la asistencia debe concederse de todos modos. En cambio, cuando la Parte requirente haya aceptado una condición determinada, quedará vinculada por ella. En virtud del párrafo 7.b, la Parte requerida que haya suministrado información o material sujeto a una condición con arreglo al párrafo 6, podrá, con el fin de verificar si se ha cumplido dicha condición, exigir a la Parte requirente que explique el uso que ha hecho de dicha información o material; con todo, se entiende que la Parte requirente no podrá exigir un control demasiado gravoso. (Véanse los párrafos 279 y 280 del Informe explicativo del Convenio).

Sección 4 - Procedimientos relativos a la asistencia mutua en caso de emergencia

Artículo 10 - Asistencia mutua en caso de emergencia

171. El artículo 10 del presente Protocolo tiene por objeto establecer un procedimiento rápido y expedito para las solicitudes de asistencia mutua formuladas en caso de emergencia. La emergencia se define en el artículo 3, párrafo 2.c, y se explica en los párrafos 41 y 42 del presente Informe explicativo.

172. El artículo 10 del presente Protocolo se limita a los casos de emergencia que justifican esa acción rápida expedita, por lo que difiere del artículo 25, párrafo 3, del Convenio, que prevé la presentación de solicitudes de asistencia mutua por medios rápidos de comunicación en casos de urgencia que no alcanzan el nivel de emergencia, con arreglo a la definición de este término. En otras palabras, el artículo 25, párrafo 3, tiene un alcance más amplio que el del artículo 10 del presente Protocolo, ya que abarca situaciones no contempladas en el artículo 10, tales como: los riesgos permanentes pero no inminentes para la vida o la seguridad de las personas; la posible destrucción de pruebas que pueda resultar de la demora; una fecha de juicio que se aproxima rápidamente, u otros tipos de situaciones de urgencia. Si bien el mecanismo del artículo 25, párrafo 3, contempla un método más rápido para transmitir y dar respuesta a una solicitud, las obligaciones en caso de emergencia en virtud del artículo 10 del presente Protocolo son considerablemente mayores; es decir, cuando existe un riesgo significativo e inminente para la vida o la seguridad de una persona física, el proceso deberá ser aún más acelerado (véanse los ejemplos de casos de emergencia en el párrafo 42 de este Informe explicativo).

Párrafo 1

173. En virtud del párrafo 1, al formular una solicitud en caso de emergencia, la Parte requirente deberá determinar que se trata de una emergencia en el sentido del artículo 3, párrafo 2.c, incluir en su solicitud una descripción de los hechos que así lo demuestren, y explicar la manera en que la asistencia solicitada es necesaria para hacer frente a la emergencia, además de otra información que deba figurar en la solicitud en virtud del tratado aplicable o del derecho interno de la Parte requerida. A este respecto, cabe recordar que, en virtud del artículo 25, párrafo 4, del Convenio, la ejecución de las solicitudes de asistencia mutua generalmente "estará sujeta a las condiciones previstas en la legislación nacional de la Parte requerida o en los tratados de asistencia

mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación". Quienes participaron en la redacción del Protocolo entendieron que ello también se aplica a las solicitudes de asistencia mutua en caso de emergencia en virtud del presente Protocolo.

Párrafo 2

174. El párrafo 2 dispone que la Parte requerida aceptará la solicitud de asistencia mutua en formato electrónico. Antes de aceptarla, la Parte requerida podrá condicionar la aceptación de la solicitud al cumplimiento por la Parte requirente de los niveles adecuados de seguridad y autenticación. En lo que respecta al requisito de seguridad que figura en este párrafo, las Partes podrán decidir entre ellas si existe la necesidad de protecciones de seguridad especiales (incluido el cifrado) que pudieran ser indispensables en un caso especialmente delicado.

Párrafo 3

175. Cuando la Parte requerida necesite información adicional para llegar a la conclusión de que existe una emergencia en el sentido del artículo 3, párrafo 2.c, y/o que se han cumplido los demás requisitos en materia de asistencia mutua, el párrafo 3 exige que la Parte recabe la información adicional de forma expedita a la mayor brevedad. Del mismo modo, el párrafo 3 exige a la Parte requirente que presente también la información complementaria de forma expedita a la mayor brevedad. Por lo tanto, ambas Partes deben hacer todo lo posible para evitar pérdidas de tiempo que pudieran contribuir inadvertidamente a un resultado trágico.

Párrafo 4

176. Con arreglo al párrafo 4, una vez presentada la información necesaria para dar cumplimiento a la solicitud, la Parte requerida deberá responder de forma rápida y expedita. En general, ello implica acelerar rápidamente la obtención de órdenes judiciales que obliguen al proveedor a aportar datos que constituyan una prueba del delito, así como la notificación de la orden al proveedor. Empero, las demoras ocasionadas por los tiempos de respuesta del proveedor para dar cumplimiento a dichas órdenes no deberán atribuirse a las autoridades del Estado requerido.

Párrafo 5

177. En virtud del párrafo 5, todas las Partes deberán garantizar que los miembros de su autoridad central de asistencia mutua, u otras autoridades responsables de dar respuesta a las solicitudes de asistencia mutua, estén

disponibles las 24 horas del día y los siete días de la semana, en caso de que sea necesario presentar solicitudes de emergencia fuera del horario normal de trabajo. A este respecto, cabe recordar que la Red 24/7 establecida en virtud del artículo 35 del Convenio principal está disponible para coordinar con las autoridades responsables de la asistencia mutua. La obligación establecida en este párrafo no requiere que la autoridad central, u otras autoridades responsables den respuesta a las solicitudes de asistencia mutua, disponga de personal y esté operativa las 24 horas del día. Más bien, esa autoridad deberá poner en práctica procedimientos que garanticen que se puede contactar con su personal cuando sea necesario examinar solicitudes de casos de emergencia fuera del horario normal de trabajo. El T-CY realizará esfuerzos de manera informal para mantener un directorio de dichas autoridades.

Párrafo 6

178. El párrafo 6 proporciona la base para que las autoridades centrales, u otras autoridades responsables de la asistencia mutua, determinen de común acuerdo un canal alternativo para la transferencia de la información o las pruebas pertinentes, lo que puede incluir tanto el modo de transmisión como las autoridades a cargo de la transferencia de la información. Por lo tanto, en lugar de transmitir la información o las pruebas que se envían en respuesta a la solicitud de la Parte requirente a través del canal de la autoridad central por el que habitualmente transita la información o las pruebas relativas a la ejecución de la solicitud de la Parte requirente, las Partes podrán decidir de común acuerdo valerse de un canal diferente a fin de acelerar la transmisión, mantener la integridad de las pruebas o por otra razón. Por ejemplo, en caso de emergencia, las autoridades podrán decidir la transmisión directa de las pruebas a una autoridad de investigación o fiscal de la Parte requirente que vaya a utilizarlas, en lugar de enviarlas a través de la cadena de autoridades por la que normalmente transitarían. Asimismo, las autoridades podrán decidir, por ejemplo, que las pruebas físicas sean objeto de un tratamiento especial con el fin de poder descartar toda posible impugnación en procedimientos judiciales posteriores si se alegase que las pruebas pudieran haber sufrido alteración o contaminación. Asimismo, podrán decidir de común acuerdo la adopción de medidas procesales especiales para la transmisión de pruebas confidenciales.

Párrafo 7

179. En lo que respecta a los procedimientos que rigen este artículo, existen dos posibilidades, reflejadas en los párrafos 7 y 8. El párrafo 7 del artículo 10

dispone que cuando las Partes requirente y requerida no estén mutuamente vinculadas por un acuerdo o convenio de asistencia mutua aplicable sobre la base de la legislación uniforme o recíproca en vigor entre las Partes, éstas aplicarán los procedimientos definidos en los párrafos especificados de los artículos 27 y 28 del Convenio (que rigen la asistencia mutua en ausencia de un tratado).

Párrafo 8

180. El párrafo 8 dispone que cuando las Partes interesadas estén mutuamente vinculadas por un acuerdo o convenio aplicable, el artículo 10 se complementará con las disposiciones de ese acuerdo o convenio, a menos que las Partes interesadas decidan de común acuerdo aplicar en lugar de las mismas alguna o todas las disposiciones del Convenio a las que se hace referencia en el párrafo 7.

Párrafo 9

181. Por último, el párrafo 9 dispone que las Partes en el presente Protocolo podrán formular una declaración en que se disponga la posibilidad del envío de solicitudes directamente entre fiscales u otras autoridades judiciales. En algunas Partes, esos cauces directos entre autoridades judiciales están bien establecidos y pueden representar un medio eficiente para acelerar aún más la formulación y ejecución de las solicitudes. La transmisión de las solicitudes en caso de emergencia a través del punto de contacto de la Red 24/7 de la Parte o por conducto de la Organización Internacional de Policía Criminal (INTERPOL) es útil no sólo para reducir cualquier retraso sino también para aumentar los niveles de seguridad y autenticación. No obstante, en algunas Partes, el envío de una solicitud directamente a una autoridad judicial de la Parte requerida sin la participación y aprobación de la autoridad central podría ser contraproducente ya que, sin la orientación y/o aprobación de su autoridad central, la autoridad receptora podría no estar facultada para actuar de forma independiente, o podría no estar familiarizada con el procedimiento pertinente. Por lo tanto, cada Parte deberá formular una declaración que permita el envío de las solicitudes por canales que no forman parte de su autoridad central.

Sección 5 - Procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables

182. Tal y como se establece en el artículo 5, párrafo 5, esta sección, referente a los artículos 11 y 12, se aplicará "cuando no exista un tratado o acuerdo

de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Partes requirente y requerida. Las disposiciones de la sección 5 no se aplicarán cuando exista dicho tratado o acuerdo, salvo en lo dispuesto en el artículo 12, párrafo 7. No obstante, las Partes interesadas podrán decidir de común acuerdo aplicar las disposiciones de la sección 5 en lugar de las mismas, si el tratado o acuerdo no lo prohíbe". Esto concuerda con los criterios del artículo 27 del Convenio.

183. Entre algunas Partes del presente Protocolo, la temática de los artículos 11 y 12 ya está regulada por los términos de tratados de asistencia mutua (por ejemplo, el Segundo Protocolo Adicional al Convenio Europeo de Asistencia Judicial en Materia Penal (STE nº 182); o el Acuerdo de asistencia judicial entre la Unión Europea y los Estados Unidos de América). Los tratados de asistencia mutua, como el STE nº 182, también pueden ofrecer más detalles sobre las circunstancias, condiciones y procedimientos en los que puede tener lugar dicha cooperación.

184. Aunque quienes participaron en la redacción tuvieron en cuenta esos tratados, los artículos 11 y 12 del presente Protocolo contienen términos que difieren de disposiciones análogas de otros tratados de asistencia mutua.

185. Si bien los términos del STE nº 182 seguirán aplicándose entre las Partes en el mismo, en el presente Protocolo se consideró apropiado regular esos dos artículos en el presente Protocolo de una manera que difiere en algunos aspectos por las siguientes razones:

- El número de países que han firmado el STE nº 182 difiere del de las Partes en el Convenio sobre la Ciberdelincuencia y, por lo tanto, sus disposiciones no se aplican a la cooperación entre todas las Partes del Convenio sobre la Ciberdelincuencia. El STE nº 182 se negoció para satisfacer las necesidades de los Estados miembros del Consejo de Europa, y no los requisitos y sistemas jurídicos y las necesidades de todas las Partes en el Convenio sobre la Ciberdelincuencia, aunque, en principio, el Convenio Europeo de Asistencia Judicial en Materia Penal (STE núm. 30) y sus Protocolos están abiertos a la adhesión de los Estados no miembros del Consejo de Europa previa invitación del Comité de Ministros.
- Las disposiciones en materia de asistencia mutua del presente Protocolo tienen un ámbito de aplicación material específico, ya que se aplican a "investigaciones o procedimientos penales específicos relativos a infracciones penales relacionadas con sistemas y datos informáticos, y a la obtención de pruebas en forma electrónica de un delito penal"

(artículo 2). Habida cuenta de los problemas particulares en este tipo de investigación o procedimiento – tales como la volatilidad de los datos, las cuestiones relativas a la territorialidad y la jurisdicción, y el volumen de solicitudes - las disposiciones análogas del STE nº 182 podrían no ser siempre aplicables de la misma manera.

– Quienes participaron en la redacción reconocieron que "como el Convenio se aplica a Partes de sistemas jurídicos y culturas muy diferentes, no es posible especificar en detalle las condiciones y salvaguardias aplicables a cada poder o procedimiento" (véase el párrafo 145 del Informe explicativo del Convenio). En cambio, las Partes deberán velar por que esas condiciones y salvaguardias brinden "la adecuada protección de los derechos y las libertades humanas" y apliquen "las normas comunes [y] las salvaguardias mínimas a las que las Partes... deben adherir", incluidas "las salvaguardias que se deriven de las obligaciones contraídas por una Parte en virtud de los instrumentos internacionales aplicables en materia de derechos humanos" (véase el párrafo 145 del Informe explicativo del Convenio). Véase el artículo 13 de este Protocolo (en el que se incorpora el artículo 15 del Convenio). Por lo tanto, a diferencia de las disposiciones del STE nº 182 - por ejemplo, el artículo 9 sobre la "audiencia por videoconferencia"- que prescribe procedimientos y salvaguardias específicos a que deben atenerse las Partes en el STE nº 182, las disposiciones correspondientes de este Protocolo brindan a las Partes mayor flexibilidad en materia de aplicación. Por ejemplo, los procedimientos y condiciones que rigen el funcionamiento de los equipos conjuntos de investigación serán los acordados por las autoridades competentes de las Partes (véase el artículo 12, párrafo 2) y, con respecto a las videoconferencias, una Parte requerida podrá exigir condiciones y salvaguardias concretas cuando permita la toma de testimonio o declaración de un sospechoso o acusado por videoconferencia (véase el artículo 11, párrafo 8). En la medida prevista en esos artículos, las Partes también podrán decidir no prestar cooperación si no se cumplen sus requisitos en cuanto a las condiciones y salvaguardias.

186. Los artículos 11 y 12 del presente Protocolo se aplicarán únicamente en ausencia de otros tratados o acuerdos de asistencia mutua basados en la legislación uniforme o recíproca en vigor - a menos que las Partes interesadas decidan de común acuerdo aplicar en su lugar alguna o todas sus disposiciones, si el tratado o acuerdo no lo prohíbe. No obstante, el artículo 12, párrafo 7 se aplica independientemente de que exista o no un tratado o

acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Partes interesadas.

Artículo 11 - Videoconferencia

187. El artículo 11 aborda principalmente el empleo de la tecnología de videoconferencia para tomar testimonio o declaraciones. Esa forma de cooperación puede estar prevista en los tratados bilaterales y multilaterales de asistencia mutua existentes, por ejemplo, el STE nº 182. A fin de no reemplazar las disposiciones concebidas específicamente para satisfacer los requisitos de las Partes en dichos tratados o convenios, y como se indica en los principios generales aplicables a esta sección (artículo 5, párrafo 5), el artículo 11, al igual que el artículo 12 del presente Protocolo, "se aplicará cuando no exista ningún tratado o acuerdo de asistencia mutua basado en una legislación uniforme o recíproca en vigor entre las Partes requirente y requerida. Las disposiciones de la sección 5 no se aplicarán cuando exista dicho tratado o acuerdo, salvo lo dispuesto en el párrafo 7 del artículo 12. No obstante, las Partes interesadas podrán determinar de común acuerdo la aplicación de las disposiciones de la sección 5 en lugar de las mismas, si el tratado o acuerdo no lo prohíbe."

Párrafo 1

188. El párrafo 1 autoriza el empleo de videoconferencias para la toma de testimonios y declaraciones de un testigo o perito. Este párrafo otorga a la Parte requerida potestad para aceptar o no la solicitud de asistencia mutua o establecer condiciones para prestar asistencia. Por ejemplo, una Parte puede negarse a prestar asistencia, o posponerla, por los motivos previstos en el artículo 27, párrafos 4 y 5 del Convenio. Alternativamente, cuando resulte más eficaz que la asistencia se preste de otra manera, por ejemplo mediante un formulario escrito que certifique la autenticidad de documentos oficiales o comerciales, la Parte requerida podrá optar por prestar la asistencia de esa manera.

189. Al mismo tiempo, se espera que las Partes en el presente Protocolo cuenten con la capacidad técnica básica para prestar asistencia mediante videoconferencia.

190. La realización de una videoconferencia destinada a tomar testimonio o declaración puede suscitar muchas dificultades, que pueden incluir problemas legales, logísticos y técnicos. La coordinación previa es esencial para que la videoconferencia transcurra sin contratiempos. Puede ser necesaria coordinación adicional cuando la Parte requerida establezca condiciones

como requisito previo a la realización de la videoconferencia. Por lo tanto, el párrafo 1 también exige que las Partes requirente y requerida celebren consultas cuando sea preciso para facilitar la solución de cualquier problema de este tipo que pueda presentarse. Por ejemplo, como se explica más adelante, podría ser necesario que la videoconferencia tenga que adoptar un determinado procedimiento para que el resultado sea admisible como prueba en la Parte requirente. A la inversa, la Parte requerida podría tener que aplicar sus propios requisitos legales en determinados aspectos (por ejemplo, la prestación de juramento por parte del testigo o el asesoramiento acerca de sus derechos). Además, la Parte requerida podría exigir que su(s) funcionario(s) esté(n) presente(s) en la videoconferencia en algunas o todas las situaciones, ya sea para presidir el procedimiento o para garantizar el respeto de los derechos de la persona a la que se le toma declaración o testimonio. A este respecto, las consultas pueden poner de manifiesto que algunas Partes requeridas exigen que su funcionario que participe en la videoconferencia pueda intervenir, interrumpir o detener la audiencia en caso de que se planteen dudas acerca de su adecuación a su legislación nacional, mientras que otras Partes pueden permitir que la videoconferencia transcurra sin la participación de sus funcionarios en algunas circunstancias. Como ejemplo adicional, las Partes requirentes pueden pedir salvaguardias especiales con respecto a testigos cuya seguridad pueda estar en peligro, los niños testigos, y casos similares. Esas cuestiones deben ser discutidas y resueltas de antemano. En algunos casos, el deseo formulado por la Parte requerida para adoptar un determinado procedimiento puede entrar en conflicto con las leyes de la Parte requirente para facilitar la utilización del testimonio o declaración en el juicio. En tales casos, las Partes deberán hacer todo lo posible para tratar de encontrar soluciones creativas que satisfagan las necesidades de ambas. Además, las Partes deberán discutir de antemano, para facilitar la resolución de problemas tales como la forma de gestionar las objeciones o reclamaciones de privilegio o inmunidad que plantee la persona o su abogado, o el empleo durante la videoconferencia de pruebas documentales o de otro tipo. Por otra parte, podrían ser necesarios procedimientos específicos debido a las condiciones impuestas para la realización de la videoconferencia. Deberán examinarse también cuestiones logísticas como, por ejemplo, determinar si corresponderá a la Parte requirente o la Parte requerida encargarse de la interpretación y la grabación del testimonio o la declaración durante la videoconferencia, y garantizar la coordinación técnica para dar inicio y mantener la transmisión y la disponibilidad de canales alternativos de comunicación en caso de interrupción de la transmisión.

Párrafo 2

191. El párrafo 2 aborda una serie de mecanismos de procedimiento y otros mecanismos conexos que rigen esta forma de cooperación (además de otros procedimientos y requisitos aplicables establecidos en los párrafos restantes del presente artículo), que han sido tomados o adaptados del Convenio. El párrafo 2 se divide en dos subpárrafos.

192. Habida cuenta de que la videoconferencia es una forma de asistencia mutua, el párrafo 2.a establece que las autoridades centrales de la Parte requerida y de la Parte requirente se comunicarán directamente entre sí a efectos de la aplicación de este artículo. Dado que este artículo sólo se aplica en ausencia de un acuerdo o convenio de asistencia mutua, sobre la base de la legislación uniforme o recíproca en vigor. Por "autoridad central" se entenderá la autoridad o autoridades designadas en virtud del artículo 27, párrafo 2.a del Convenio (véase el artículo 3, párrafo 2.a, del presente Protocolo y el párrafo 38 del Informe explicativo.

193. El párrafo 2.a de este artículo dispone también que la Parte requerida podrá aceptar una solicitud de videoconferencia en formato electrónico, y exigir niveles adecuados de seguridad y autenticación antes de aceptar la solicitud.

194. El párrafo 2.b exige (al igual que el artículo 27, párrafo 7, del Convenio) que la Parte requerida informe a la Parte requirente de sus razones para no dar curso a una solicitud o para retrasar su ejecución. Como se indica en el párrafo 192 *supra*, dichas comunicaciones deberán transitar por los canales de la autoridad central. Por último, el párrafo 2.b establece que el artículo 27, párrafo 8 (relativo a la confidencialidad de una solicitud de asistencia mutua en ausencia de un tratado), y el artículo 28, párrafos 2 a 4 del Convenio (relativos a la confidencialidad del material en respuesta a la solicitud y a las restricciones de la utilización en ausencia de un tratado), se aplican al artículo sobre videoconferencias.

Párrafo 3

195. Dado que una videoconferencia puede necesitar que los funcionarios judiciales y auxiliares de una Parte requirente estén disponibles para participar en la toma de testimonio o declaración en la Parte requerida, distantes entre sí muchas zonas horarias, es fundamental que la persona que va a declarar comparezca en el lugar y la hora previstos. En virtud del párrafo 3, cuando la Parte requerida preste asistencia en virtud del presente artículo, deberá procurar obtener la presencia de la persona cuyo testimonio o declaración se ha solicitado. La mejor manera de hacerlo puede depender de las circunstancias

del caso, de la legislación interna de la Parte requerida y de si, por ejemplo, se confía en que la persona comparecerá voluntariamente a la hora concertada. En cambio, para garantizar la comparecencia de la persona, podría ser aconsejable que la Parte requerida emitiese una orden o citación que obligase a la persona a comparecer, y este párrafo la autoriza a proceder de esa manera, con arreglo a las garantías establecidas en su derecho interno.

Párrafo 4

196. El procedimiento relativo a la realización de las videoconferencias se establece en el párrafo 4. El objetivo principal es proporcionar a la Parte requirente el testimonio o la declaración en una forma que permita su utilización como prueba en su investigación y sus actuaciones. Por ello, se aplicarán los procedimientos solicitados por la Parte requirente, a menos que ello sea incompatible con la legislación de la Parte requerida, incluidos los principios jurídicos aplicables de la Parte requerida no codificados en su legislación. Por ejemplo, durante la videoconferencia, el procedimiento preferible sería que la Parte requerida permitiera a las autoridades de la Parte requirente interrogar directamente a la persona de la que se solicita testimonio o declaración. El fiscal, juez de instrucción o investigador de la Parte requirente será quien conozca más a fondo la investigación o el proceso penal y, por lo tanto, quien mejor sepa qué preguntas son más útiles para la investigación o el proceso, así como la manera más adecuada de formularlas para que se ajusten a la legislación de la Parte requirente. En ese caso, la autoridad de la Parte requerida que participe en la audiencia intervendrá únicamente si fuera necesario porque la autoridad de la Parte requirente ha procedido de forma incompatible con la legislación de la Parte requerida. En ese caso, la Parte requerida podrá desautorizar las preguntas, encargarse del interrogatorio o tomar otras medidas que resulten apropiadas con arreglo a su legislación y a las circunstancias de la videoconferencia. La expresión "incompatible con la legislación de la Parte requerida" no abarca las situaciones en las que el procedimiento es simplemente diferente al de la Parte requerida, lo que suele ocurrir. Se trata más bien de situaciones en las que el procedimiento es contrario o inviable en virtud de la legislación de la Parte requerida. En esos casos, o cuando la Parte requirente no solicite ningún procedimiento específico, el procedimiento por defecto será el aplicable en virtud de la legislación de la Parte requerida. Si la aplicación de la legislación de la Parte requerida plantea un problema a la Parte requirente, por ejemplo, en lo que respecta a la admisibilidad en el juicio del testimonio o de la declaración, las Partes requirente y requerida podrán tratar de llegar a un acuerdo sobre otro

procedimiento diferente que satisfaga a la Parte requirente pero que evite el problema en virtud de la legislación de la Parte requerida.

Párrafo 5

197. El párrafo 5, relativo a la pena o sanción por declaración falsa, negativa a responder y otras faltas prohibidas por el derecho interno de la Parte requerida, tiene la finalidad de proteger la integridad del proceso de prestación de testimonio o declaración cuando el testigo se encuentra físicamente en un país distinto de aquel en el que tiene lugar el proceso penal. En la medida en que la Parte requerida haya impuesto a la persona la obligación de testificar o de declarar con veracidad o le haya prohibido determinadas conductas (por ejemplo, perturbar el proceso), el testigo quedará sujeto a las consecuencias establecidas en la jurisdicción en la que se encuentre. En tales casos, la Parte requerida deberá poder aplicar la sanción que sería aplicable si dicha conducta hubiera tenido lugar en el curso de sus procedimientos internos. Se aplicará sin menoscabo de cualquier jurisdicción de la Parte requirente. Este requisito supone un incentivo adicional para que el testigo declare, testifique con veracidad y no incurra en una conducta prohibida. Si en el procedimiento interno de la Parte requerida no existe una sanción aplicable (por ejemplo, a una declaración falsa de un acusado), no es necesario establecer ninguna sanción para tal conducta cometida en el transcurso de una videoconferencia. Esta disposición será útil sobre todo para garantizar el enjuiciamiento de un testigo que preste falso testimonio pero que no pueda ser extraditado para ser enjuiciado en la Parte requirente debido, por ejemplo, a la prohibición de extradición de nacionales por parte de la Parte requerida.

Párrafo 6

198. El párrafo 6 establece las normas relativas al reparto de los gastos relacionados con las videoconferencias. Por regla general, todos los gastos relacionados con la realización de una videoconferencia corren a cargo de la Parte requerida, a excepción de: i) los honorarios de un perito; ii) los gastos de traducción, interpretación y transcripción, y iii) los gastos que sean tan importantes como para tener carácter extraordinario. Los gastos de viaje y de pernoctación en la Parte requerida no suelen ser elevados, por lo que dichos gastos, si los hubiere, suelen ser absorbidos por la Parte requerida. No obstante, las normas relativas a los gastos podrán ser modificadas mediante acuerdo entre las Partes requirente y requerida. Por ejemplo, si la Parte requirente estipula la necesidad de contar con la presencia de un intérprete, o de

tener servicios de transcripción de la videoconferencia en su país, podría no tener que pagar a la Parte requerida para que preste dichos servicios. Cuando la Parte requerida prevea costes extraordinarios para la prestación de asistencia, de conformidad con el párrafo 6.b, la Parte requirente y la Parte requerida se consultarán antes de ejecutar la solicitud para determinar si la Parte requirente puede asumir dichos gastos y, si no pudiera asumirlos, la manera de evitarlos.

Párrafo 7

199. Si bien el párrafo 1 autoriza expresamente el empleo de la tecnología de videoconferencia para la toma de testimonios o declaraciones, el párrafo 7.a establece que las disposiciones del artículo 11 podrán aplicarse para la realización de audioconferencias cuando así se decida de común acuerdo. Además, el párrafo 7.b dispone que, cuando así lo acuerden las Partes requirente y requerida, la tecnología podrá utilizarse para "fines, o audiencias distintos..., incluso para fines de identificación de personas u objetos". Por lo tanto, si fuera acordado mutuamente, las Partes requirente y requerida podrán contemplar la posibilidad de utilizar tecnología de videoconferencia para oír o realizar actuaciones relativas a un sospechoso o acusado (cabe señalar que algunas Partes pueden considerar que un sospechoso o acusado es un "testigo", por lo que la toma de testimonio o declaración de esa persona ya estaría protegida por el párrafo 1 del presente artículo). Cuando el párrafo 1 no sea aplicable, el párrafo 7 otorga autoridad legal para permitir la utilización de la tecnología en tales casos.

Párrafo 8

200. El párrafo 8 aborda la situación en la que la Parte requerida opta por permitir la audiencia de un sospechoso o acusado, por ejemplo, a efectos de prestar testimonio o declaración o para la entrega de notificaciones u otras medidas procesales. Al igual que tiene potestad para permitir la comparecencia por videoconferencia de un testigo o perito ordinario, la Parte requerida tiene facultades discrecionales con respecto a un sospechoso o acusado. Asimismo, además de cualquier otra condición o restricción que una Parte requerida pueda imponer para permitir la realización de una videoconferencia, la legislación interna de una Parte podrá exigir condiciones específicas con respecto a la audiencia de sospechosos o acusados. Por ejemplo, la legislación de una Parte puede exigir el consentimiento del sospechoso o acusado para prestar testimonio o declaración, o la legislación de una Parte puede prohibir o restringir la utilización de videoconferencias para las notificaciones u otras

medidas procesales. Por tanto, el párrafo 8 tiene por objeto hacer hincapié en el hecho de que los procedimientos dirigidos a un sospechoso o acusado pueden suscitar la necesidad de condiciones o salvaguardias suplementarias a las que de otra manera podrían plantearse.

Artículo 12 - Equipos conjuntos de investigación e investigaciones conjuntas

201. Dado el carácter transnacional de la ciberdelincuencia y de las pruebas electrónicas, las investigaciones y los procesos relacionados con la ciberdelincuencia y las pruebas electrónicas suelen tener vínculos con otros Estados. Los equipos conjuntos de investigación pueden ser un medio eficaz de cooperación o coordinación operativa entre dos o más Estados. El artículo 12 proporciona una base para tales formas de cooperación.

202. La experiencia ha demostrado que cuando un Estado investiga un delito relacionado con la ciberdelincuencia que tiene una dimensión transfronteriza, o para el que es necesario obtener pruebas electrónicas, la investigación puede enriquecerse con la participación de las autoridades de otros Estados que también investigan la misma conducta o una conducta conexa, o cuando la coordinación se considere útil por otras razones.

203. Como se expone en el artículo 5 del presente Protocolo y en los párrafos 182 a 186 del Informe explicativo, las disposiciones del artículo 12 no se aplicarán cuando exista un tratado o acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Parte requirente y requerida, a menos que las Partes interesadas determinen de común acuerdo aplicar en lugar de las mismas un aspecto o la totalidad del resto del presente artículo, si el tratado o acuerdo no lo prohíbe. Como se explica a continuación, el párrafo 7 se aplica independientemente de que exista o no un tratado o acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Partes interesadas.

Párrafo 1

204. El párrafo 1 establece que las autoridades competentes de dos o más Partes pueden acordar la creación de un equipo conjunto de investigación (ECI) cuando consideren que puede ser especialmente útil. Un ECI se establece de mutuo acuerdo. Los términos "mutuo acuerdo", "acuerdo" y "acordar" - tal y como se utilizan en este artículo - no deben entenderse en el sentido de que sea necesario un acuerdo vinculante con arreglo al derecho internacional.

205. En este artículo se emplean dos términos relacionados: "autoridades competentes" y "autoridades participantes". Cada Parte determina qué autoridades son competentes - es decir, las "autoridades competentes" – para establecer un ECI. Algunas Partes pueden autorizar la concertación de este tipo de acuerdo por parte de diversos funcionarios, como fiscales, jueces de instrucción u otros altos funcionarios responsables de hacer cumplir la ley que estén encargados de dirigir investigaciones o procedimientos penales. Otras Partes pueden determinar que el establecimiento de este tipo de acuerdo corresponde a la autoridad central, es decir, a la dependencia normalmente responsable de las cuestiones de asistencia mutua. La decisión acerca de cuáles serán las autoridades que participarán de hecho en el equipo conjunto de investigación - las "autoridades participantes" – corresponderá también a las Partes respectivas.

Párrafo 2

206. El párrafo 2 establece que los procedimientos y condiciones que rijan el funcionamiento de los equipos conjuntos de investigación, tales como sus fines específicos; su composición; sus funciones; su duración y cualquier período de prórroga; su ubicación; su organización; las condiciones de recopilación, transmisión y utilización de la información o de las pruebas; las condiciones de confidencialidad, y las condiciones de participación de las autoridades de una Parte en las actividades de investigación que tengan lugar en el territorio de la otra Parte, serán los que acuerden dichas autoridades competentes. En particular, durante la preparación del acuerdo, las Partes interesadas tal vez deseen examinar las condiciones para denegar o restringir la utilización de la información o de las pruebas, incluso, por ejemplo, los motivos establecidos en el artículo 27, párrafos 4 o 5 del Convenio, así como el procedimiento que se adoptará si la información o las pruebas son necesarias para otros fines distintos de aquellos para los que se ha concertado el acuerdo (incluida la utilización de la información o de las pruebas por parte de la acusación o la defensa en otro caso, o cuando éstas puedan ser necesarias para prevenir una emergencia, tal como se define en el artículo 3, párrafo 2.c, es decir, una situación en la que exista un riesgo significativo e inminente para la vida o la seguridad de una persona física). Se alienta a las Partes a que especifiquen en el acuerdo los límites de las facultades de los funcionarios participantes de una Parte que se encuentren físicamente presentes en el territorio de otra Parte. También se anima a las Partes a que en el acuerdo permitan la transmisión electrónica de la información o las pruebas reunidas.

207. Se espera que las Partes generalmente determinarán de común acuerdo esos procedimientos y condiciones por escrito. En todo acuerdo, debe tenerse en cuenta el nivel de detalle necesario. Un texto simplificado puede proporcionar el nivel de precisión necesario para las circunstancias previsibles, con la posibilidad de añadir disposiciones complementarias si las circunstancias futuras requiriesen mayor precisión. Las Partes contemplarán el alcance geográfico y la duración del acuerdo por el que se establece el equipo conjunto de investigación y tendrán en cuenta que podría ser necesario modificarlo o ampliarlo a medida que se conozcan nuevos hechos.

208. La información o las pruebas utilizadas en el marco del equipo conjunto de investigación podrán incluir datos personales tales como información relativa a los abonados, datos sobre el tráfico o datos sobre el contenido. Al igual que ocurre con otras medidas de cooperación en virtud del presente Protocolo, el artículo 14 se aplica a la transferencia de datos personales con arreglo a los equipos conjuntos de investigación.

209. Como suele ocurrir en lo que respecta a toda la información o las pruebas recibidas por una Parte en virtud del presente Protocolo, las normas probatorias aplicables de esa Parte regirán la admisibilidad de la información o las pruebas en los procedimientos judiciales.

Párrafo 3

210. El párrafo 3 permite a una Parte hacer una declaración en el momento de la firma del presente Protocolo, o al depositar su instrumento de ratificación, aceptación o aprobación, en que señale que su autoridad central debe ser signataria del acuerdo por el que se establece el equipo o estar de otra manera de acuerdo con él. Esa disposición se adoptó por varias razones. En primer lugar, varias Partes estiman que los equipos conjuntos de investigación son una forma de asistencia mutua; en otras Partes, las autoridades centrales responsables de la asistencia mutua pueden contribuir a garantizar el cumplimiento de los requisitos jurídicos internos aplicables cuando las autoridades competentes (que pueden ser fiscales o policías con una experiencia relativamente limitada en cuestiones de cooperación internacional) preparan un acuerdo de ECI con arreglo a este artículo. La experiencia de una autoridad central con acuerdos internacionales que rigen la asistencia mutua y otras formas de cooperación internacional (incluido el presente Protocolo) también puede representar un valioso aporte para garantizar el cumplimiento de los requisitos del Protocolo. Por último, si una Parte ha efectuado la declaración contemplada en el presente párrafo, las autoridades

de otras Partes que deseen establecer un equipo conjunto de investigación con la Parte declarante estarán advertidas de que es necesario que la autoridad central de la Parte declarante firme el acuerdo, o esté de acuerdo con él, para que sea válido con arreglo al Protocolo. Esto brinda protección contra el establecimiento de un equipo conjunto de investigación que no cuente con la debida autorización o que no cumpla con la normativa legal aplicable de la Parte declarante.

Párrafo 4

211. En virtud del párrafo 4, las autoridades competentes designadas por las Partes con arreglo al párrafo 1 y las autoridades participantes mencionadas en el párrafo 2 se comunicarán normalmente entre sí de forma directa en aras de la eficiencia y la eficacia. No obstante, cuando circunstancias excepcionales requiriesen una coordinación más centralizada - como en casos con ramificaciones especialmente graves o en situaciones que planteen problemas particulares de coordinación - podrán aceptarse otros canales de comunicación idóneos. Por ejemplo, las autoridades centrales encargadas de la asistencia mutua podrían estar disponibles para ayudar a coordinar tales asuntos.

Párrafo 5

212. El párrafo 5 prevé que cuando sea necesario adoptar medidas de investigación en el territorio de una de las Partes afectadas, las autoridades participantes de esa Parte podrán solicitar a sus propias autoridades la adopción de dichas medidas. Esas autoridades determinarán si pueden adoptar la medida de investigación con arreglo a su legislación nacional. En caso de que puedan hacerlo, no será necesario que otras Partes participantes presenten una solicitud de asistencia mutua. Este es uno de los aspectos más innovadores de los equipos conjuntos de investigación. No obstante, en algunas situaciones, podría ocurrir que esas autoridades no tengan la suficiente autoridad nacional para adoptar una medida de investigación concreta en nombre de otra Parte sin antes recibir una solicitud de asistencia mutua.

Párrafo 6

213. El párrafo 6 aborda la utilización de la información o las pruebas facilitadas por las autoridades participantes de una Parte a las autoridades participantes de otra Parte. La utilización podrá denegarse o restringirse de acuerdo a lo establecido en el acuerdo mencionado en los párrafos 1 y 2. No obstante, si dicho acuerdo no establece condiciones para denegar o restringir la utilización,

será posible utilizar la información o las pruebas de la manera prevista en los párrafos del 6.a al 6.c. Las circunstancias reflejadas en el párrafo 6 se entenderán sin perjuicio de los requisitos establecidos en el artículo 14 respecto de la ulterior transferencia de la información o las pruebas a otro Estado.

214. Cabe señalar que, cuando son aplicables los párrafos del 6.a al 6.c, las autoridades participantes podrán, no obstante, decidir de común acuerdo restringir aún más la utilización de información o pruebas específicas a fin de evitar consecuencias adversas para una de sus investigaciones, ya sea antes o, especialmente, después de que se haya facilitado la información o las pruebas. Por ejemplo, incluso si la Parte que las ha recibido desea utilizar las pruebas para un fin que hubiere dado lugar a la creación del equipo mixto de investigación, su utilización podría tener un efecto adverso en la investigación llevada a cabo por la Parte que ha facilitado la información o las pruebas (por ejemplo, al revelar la existencia de la investigación a un grupo criminal, lo que podría provocar la huida de los criminales, la destrucción de las pruebas o la intimidación de los testigos). En ese caso, la Parte que entregó la información o las pruebas puede pedir a la otra Parte que acceda a no hacerla pública hasta que desaparezca ese riesgo.

215. En el párrafo 6.b, quienes participaron en la redacción aspiraban a que, en ausencia de un acuerdo que establezca condiciones para denegar o restringir la utilización de los elementos facilitados, no se exigiría el consentimiento de las autoridades que facilitaron la información o las pruebas cuando, en virtud de los principios jurídicos fundamentales de la Parte cuyas autoridades participantes la han recibido, sea necesario poner en conocimiento de la defensa o de una autoridad judicial la información o las pruebas importantes que permitan organizar una defensa eficaz en las actuaciones relativas a esos otros delitos. Aun cuando en este caso no se requiere consentimiento, la notificación de la divulgación de la información o de las pruebas para tal fin se hará sin demora injustificada. Si fuera posible, la notificación deberá hacerse antes de proceder a la divulgación, a fin de que la Parte que ha facilitado la información o las pruebas pueda prepararse para la divulgación, y de permitir a las Partes que realicen las consultas oportunas.

216. Quienes participaron en la redacción entendieron que el párrafo 6.c se refiere a circunstancias excepcionales en las que las autoridades de la Parte receptora podrían utilizar directamente la información o las pruebas para evitar una emergencia, tal como se define en el artículo 3, párrafo 2.c del presente Protocolo. La seguridad de una persona física implica lesiones corporales graves. El concepto de "riesgo significativo e inminente para la vida o la seguridad de

cualquier persona física" se explica en mayor detalle en el Informe explicativo en el párrafo 42, en que también se presentan ejemplos de tales situaciones. Quienes participaron en la redacción consideraron que ese concepto abarca los casos en los que una amenaza significativa e inminente a bienes o redes representa un riesgo para la vida o la seguridad de una persona física. En caso de que se utilice información o pruebas con arreglo al párrafo 6.c, se notificará sin demora injustificada a las autoridades participantes de la Parte que haya facilitado la información o las pruebas, a menos que se determine lo contrario de mutuo acuerdo. Por ejemplo, las autoridades participantes podrán determinar que se notifique a la autoridad central.

Párrafo 7

217. Por último, cabe recordar de manera general que existe una larga historia de actividades de cooperación internacional sobre una base *ad hoc* entre organismos encargados de hacer cumplir la ley en las que un equipo de fiscales y/o investigadores de un país coopera con sus homólogos extranjeros en una investigación concreta, actividades que no están comprendidas en el marco de un equipo conjunto de investigación. El párrafo 7 contempla esas actividades de cooperación internacional y brinda un fundamento jurídico para dar inicio a una investigación conjunta a falta de un acuerdo como el mencionado en los párrafos 1 y 2, en caso de que una Parte requiera esa base jurídica. El presente párrafo se aplicará independientemente de que exista o no un tratado o acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Partes interesadas. Al igual que ocurre con todas las medidas en virtud del presente Protocolo, las investigaciones conjuntas previstas en el párrafo 7 están sujetas a las condiciones y salvaguardias del capítulo III.

Capítulo III - Condiciones y salvaguardias

Artículo 13 - Condiciones y salvaguardias

218. Sobre la base del artículo 15 del Convenio, el artículo 13 dispone que "cada Parte velará por que el establecimiento, la ejecución y la aplicación de las facultades y los procedimientos previstos en el presente Protocolo estén sujetos a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar la protección adecuada de los derechos humanos y las libertades". Dado que este artículo se basa en el artículo 15 del Convenio, la explicación de dicho artículo que figura en los párrafos 145 a 148 del Informe explicativo del Convenio es también válida para el artículo 13 del presente

Protocolo, incluido el hecho de que el principio de proporcionalidad "deberá ser aplicado por cada Parte con arreglo a los principios pertinentes de su derecho interno" (véase el párrafo 146 del Informe explicativo del Convenio).

219. Cabe señalar que, además de este artículo, otros artículos contienen importantes salvaguardias. Por ejemplo, las medidas del presente Protocolo tienen un alcance limitado, es decir, se aplicarán "a las investigaciones o procedimientos penales específicos relativos a los delitos relacionados con sistemas y datos informáticos, y a la obtención de pruebas en forma electrónica de un delito penal" (véase el artículo 2). Además, en los distintos artículos se especifica la información que se incluirá en las solicitudes, las órdenes y la información de acompañamiento que pueda contribuir a la aplicación de las salvaguardias nacionales (véase el artículo 6, párrafo 3; el artículo 7, párrafos 3 y 4; el artículo 8, párrafo 3, y el artículo 9, párrafo 3). Además, los tipos de datos que deberán divulgarse se especifican en cada artículo como, por ejemplo, en el artículo 7, que se limita a la información relativa al abonado. Asimismo, las Partes pueden formular reservas y declaraciones, por ejemplo, para restringir el tipo de información que ha de facilitarse, como en los artículos 7 y 8. Por último, cuando se transfieran datos personales en virtud del presente Protocolo, se aplicarán las garantías de protección de datos previstas en el artículo 14.

Artículo 14 - Protección de los datos personales

Párrafo 1 - Ámbito de aplicación

220. Las medidas previstas en el capítulo II del presente Protocolo implican en muchos casos la transferencia de datos personales. En vista de que muchas Partes en el presente Protocolo, a fin de cumplir sus obligaciones constitucionales o internacionales, pueden verse obligadas a garantizar la protección de los datos personales, el artículo 14 establece salvaguardias de protección de datos que permiten a las Partes cumplir esas exigencias y, por lo tanto, facilitan el tratamiento de los datos personales a los efectos del presente Protocolo.

221. De conformidad con el párrafo 1.a, cada Parte procederá a tratar los datos personales que reciba en virtud del presente Protocolo con arreglo a las salvaguardias específicas establecidas en los párrafos 2 a 15. Ello incluye los datos personales transferidos como parte de una orden o solicitud en virtud del presente Protocolo. No obstante, no se aplicarán los párrafos 2 a 15 si los términos de las excepciones articuladas en los párrafos 1.b o 1.c son aplicables.

222. La primera excepción se expone en el párrafo 1. b, que establece que "[s]i en el momento de la recepción de los datos personales en virtud del

presente Protocolo, tanto la Parte transferente como la Parte receptora están mutuamente vinculadas por un acuerdo internacional que establezca un marco global entre dichas Partes para la protección de los datos personales que sea aplicable a la transferencia de datos personales con fines de prevención, detección, investigación y enjuiciamiento de delitos penales, y que disponga que el tratamiento de los datos personales en virtud de dicho acuerdo cumple con los requisitos de la legislación sobre protección de datos de las Partes afectadas, los términos de dicho acuerdo se aplicarán, para las medidas que entren en su ámbito de aplicación, a los datos personales recibidos en virtud del Protocolo en lugar de los párrafos 2 a 15, a menos que las Partes interesadas acuerden otra cosa." En este contexto, en general, se considerará que un marco es "global" cuando abarque integralmente los aspectos de protección de datos aplicables a las transferencias de datos. Dos ejemplos de acuerdos que satisfacen lo dispuesto en el párrafo 1.b son el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), modificado por el Protocolo (STCE nº 223), y el Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales, relativo a la prevención, investigación, detección o enjuiciamiento de infracciones penales. Los términos de dichos acuerdos se aplicarán, en lugar de los párrafos 2 a 15, a las medidas comprendidas en el ámbito de aplicación de dichos acuerdos. En lo tocante a las Partes en el Convenio STE nº 108, modificado por el Protocolo STCE nº 223, ello significa que es aplicable el artículo 14, párrafo 1, tal y como se explica en los párrafos 105 a 107 del Informe explicativo de dicho Convenio. Por lo que respecta al calendario, los párrafos 2 a 15 de este artículo quedarán sin efecto sólo si las Partes están mutuamente vinculadas por el acuerdo en el momento en que se reciban los datos personales en virtud del presente Protocolo. Esto se aplica siempre y cuando el acuerdo disponga que los datos transferidos en virtud del mismo sigan siendo tratados con arreglo a los términos de dicho acuerdo.

223. La segunda excepción se enuncia en el párrafo 1.c, que dispone que, incluso si no están mutuamente vinculadas por un acuerdo del tipo descrito en el párrafo 1.b, las Partes transferente y receptora podrán determinar mutuamente que la transferencia de datos personales en virtud del presente Protocolo pueda tener lugar sobre la base de otros acuerdos o arreglos entre las Partes interesadas en lugar de los párrafos 2 a 15 del presente artículo. Esto garantiza que las Partes sigan teniendo flexibilidad para determinar las salvaguardias en materia de protección de los datos que son aplicables a las transferencias entre ellas en virtud del Protocolo. Con el fin de brindar seguridad jurídica y transparencia a las personas y a los proveedores y entidades

que participan en las transferencias de datos con arreglo a las medidas del capítulo 2, sección 2 del presente Protocolo, se alienta a las Partes a que den a conocer públicamente de manera clara su determinación mutua de que dicho acuerdo o convenio ha de regir los aspectos referentes a la protección de los datos incluidos en las transferencias de datos personales entre las Partes.

224. Quienes participaron en la redacción del Protocolo estimaron que, mediante las salvaguardias de protección de datos establecidas en los párrafos 2 a 15 de este artículo, el presente Protocolo garantiza protección adecuada para las transferencias de datos en virtud del Protocolo. A tal efecto, de acuerdo con el párrafo 1.d, se considerará que la transferencia de datos en virtud del párrafo 1.a cumple los requisitos en materia de protección de los datos personales previstos en el marco jurídico de cada una de las Partes en lo que se refiere a las transferencias internacionales de datos personales, y no será necesaria ninguna otra autorización para la transferencia con arreglo a dicho marco jurídico.

Además, en la medida en que los términos de los acuerdos descritos en el párrafo 1.b disponen que el tratamiento de los datos personales en virtud de dichos acuerdos cumple los requisitos en materia de protección de los datos personales previstos en el marco jurídico de las Partes interesadas, el párrafo 1.d hace extensiva esa aprobación a las transferencias efectuadas en virtud del presente Protocolo. Por lo tanto, este párrafo brinda seguridad jurídica para las transferencias internacionales de datos personales con arreglo a los párrafos 1.a o 1.b en respuesta a órdenes y solicitudes emitidas en virtud del presente Protocolo, a fin de garantizar un intercambio de datos eficaz y previsible. Dado que los acuerdos o convenios mencionados en el párrafo 1.c podrían no siempre ser conformes con el marco jurídico sobre protección de datos de las Partes en lo referente a las transferencias internacionales -por ejemplo, tratándose de tratados bilaterales de asistencia mutua-, con arreglo al presente Protocolo no reciben el mismo refrendo que los previstos en los párrafos 1.a o 1.b. No obstante, las Partes interesadas podrán otorgar el necesario refrendo de mutuo acuerdo.

225. Asimismo, el párrafo 1.d establece que una Parte sólo podrá denegar o impedir la transferencia de datos personales a otra Parte en virtud del presente Protocolo por motivos de protección de datos: i) en las condiciones establecidas en el párrafo 15 en relación con las consultas y suspensiones, cuando sea aplicable el párrafo 1.a; o ii) en virtud de los términos de acuerdos o convenios específicos a que se hace referencia en los párrafos 1.b o 1.c, cuando sea aplicable uno de esos párrafos.

226. Por último, el artículo 14 tiene como objeto establecer las salvaguardias adecuadas que permitan la transferencia de datos personales entre las Partes en virtud del presente Protocolo. El artículo 14 no exige la armonización de los marcos jurídicos nacionales para el tratamiento de los datos personales en general, ni del régimen pertinente al tratamiento de los datos personales a los efectos de la aplicación de la legislación penal específicamente. El párrafo 1.e. establece que no se impedirá a las Partes aplicar salvaguardias de protección de datos más estrictas que las previstas en los párrafos 2 a 15 en relación con el tratamiento, por sus propias autoridades, de los datos personales que dichas autoridades reciban en virtud del presente Protocolo. En cambio, el párrafo 1.e. no tiene por objeto permitir que las Partes impongan requisitos adicionales en materia de protección de datos para las transferencias de datos en virtud del presente Protocolo aparte de los permitidos específicamente en este artículo.

Párrafo 2 - Finalidad y utilización

227. El párrafo 2 aborda la finalidad y la utilización para los que las Partes pueden tratar los datos personales en virtud del Protocolo. El párrafo 2.a dispone que "la Parte que haya recibido datos personales ("Parte receptora") procederá a su tratamiento para los fines descritos en el artículo 2", es decir, para los fines de "investigaciones o procedimientos penales específicos relativos a los delitos relacionados con sistemas y datos informáticos" y para la "obtención de pruebas en forma electrónica de un delito penal", y en lo que respecta a las Partes en el Primer Protocolo, a "investigaciones o procedimientos penales específicos relativos a delitos penales tipificados con arreglo al Primer Protocolo". En otras palabras, las autoridades deben estar investigando o procesando una actividad delictiva específica, que es el fin legítimo para el que se pueden solicitar y procesar pruebas o información que contenga datos personales.

228. Aunque, en primera instancia, el Protocolo podrá invocarse solamente para obtener información o pruebas en una investigación o procedimiento penal específico y no para otros fines, el párrafo 2.a establece también que una Parte "no hará tratamiento adicional de los datos personales con una finalidad incompatible, y no someterá los datos a tratamiento ulterior cuando no lo permita su marco jurídico nacional". Con el fin de determinar si la finalidad del tratamiento ulterior no es incompatible con la finalidad inicial, se alienta a la autoridad competente a realizar una evaluación global de las circunstancias específicas, tales como: i) la relación entre la finalidad inicial y la finalidad ulterior (por ejemplo, cualquier vínculo objetivo); ii) las consecuencias (posibles) de la

utilización ulterior prevista para las personas afectadas, teniendo en cuenta la índole de los datos personales (por ejemplo, su sensibilidad); iii) cualquier expectativa razonable de las personas afectadas en relación con la finalidad de la utilización ulterior y con las entidades que podrían encargarse del tratamiento de los datos, y iv) la forma en que los datos serán tratados y estarán protegidos contra un uso indebido. El marco jurídico de una Parte podrá establecer además restricciones especiales en lo que respecta a otros fines para los que puedan destinarse los datos.

229. El tratamiento con fines no incompatibles incluiría normalmente la utilización de los datos en el ámbito de la cooperación internacional de conformidad con las legislaciones nacionales y los acuerdos o convenios internacionales (por ejemplo, de asistencia mutua) en la esfera del derecho penal. Asimismo, podría incluir, entre otras cosas, su utilización para determinadas funciones de la administración pública, como la presentación de informes a los órganos de supervisión; las investigaciones conexas sobre violaciones del derecho penal, civil o administrativo (incluidas las investigaciones realizadas por otros componentes de la administración pública) y sus sentencias; la divulgación exigida por órdenes judiciales nacionales; la divulgación a litigantes privados; la divulgación de cierta información al abogado de un acusado, y la divulgación directa al público o a los medios de comunicación (incluso en el contexto del acceso a las solicitudes de documentos y procedimientos judiciales públicos). Del mismo modo, podrá considerarse compatible el tratamiento posterior de los datos personales con fines de archivo en interés público y de investigación científica o histórica, o con fines estadísticos.

230. El párrafo 2.a permite además a las Partes imponer condiciones y restricciones adicionales en cuanto a la utilización de los datos personales en casos concretos, en la medida prevista en el capítulo II del presente Protocolo. No obstante, dichas condiciones no incluirán condiciones genéricas de protección de datos -es decir, que no sean específicas para el caso- con excepción de las previstas en el artículo 14. A modo de ejemplo, en virtud del párrafo 14 se aceptan diferentes sistemas de supervisión y en un caso concreto una Parte no podrá imponer como condición para la transferencia que la Parte requirente cuente con el equivalente de una autoridad especializada en materia de protección de datos.

231. Por último, el párrafo 2.b exige que, al solicitar y utilizar datos personales en virtud del Protocolo, "la Parte receptora garantizará, con arreglo a su marco jurídico interno, que los datos personales solicitados y tratados sean pertinentes y no excesivos en relación con los fines de dicho tratamiento".

Este requisito puede cumplimentarse, por ejemplo, mediante las reglas probatorias y la restricción del alcance de las órdenes de tratamiento obligatorio, los principios de necesidad y proporcionalidad, el principio de razonabilidad y las directrices y políticas internas que restringen la obtención o utilización de datos. Además, se alienta a las Partes a que, con arreglo a sus marcos jurídicos nacionales, contemplen las situaciones que puedan afectar a personas vulnerables como, por ejemplo, las víctimas o los menores.

Párrafo 3 - Calidad e integridad

232. El párrafo 3 exige a las Partes que adopten "medidas razonables para garantizar que los datos personales se mantengan con exactitud e integridad y estén tan actualizados como sea necesario y adecuado para el tratamiento legítimo de los datos personales, teniendo en cuenta los fines del tratamiento de los mismos". El contexto es importante, ya que este principio puede aplicarse de distinta manera en diferentes situaciones. Por ejemplo, el principio se aplicaría de forma distinta para los procedimientos penales que para otros fines.

233. En lo que respecta a las investigaciones y los procedimientos penales, no deberá entenderse que el párrafo 3 exija a las autoridades policiales y judiciales que alteren la información - incluso si ésta fuera inexacta o incompleta - que pueda constituir una prueba en una causa penal, ya que la inexactitud de los datos puede ser fundamental para el procesamiento del delito (por ejemplo, en los casos de fraude), y también socavaría la presunción de inocencia del acusado si las autoridades modificaran una prueba obtenida en virtud del Protocolo.

234. En muchas situaciones, cuando existan dudas sobre la fiabilidad de los datos personales, ello deberá indicarse claramente. Por ejemplo, en la medida en que la información o las pruebas que se han recibido en virtud del Protocolo sean utilizadas para rastrear conductas delictivas pasadas, los procedimientos aplicables deberían incluir medios para corregir o memorizar los errores en la información (por ejemplo, modificando o complementando la información original), y para actualizar, modificar o complementar datos poco fiables o desactualizados, con el fin de minimizar el riesgo de que las autoridades adopten medidas policiales inadecuadas y potencialmente adversas debido a la calidad deficiente de los datos (por ejemplo, la detención de la persona equivocada, o el arresto de una persona que reposa en una comprensión errónea de su conducta). Se alienta a las Partes a que adopten medidas razonables para garantizar que, cuando se determine que los datos facilitados a otra autoridad

o recibidos de ella son erróneos o no están actualizados, la otra autoridad sea informada lo más pronto posible para que efectúe las correcciones necesarias correspondientes habida cuenta de los fines del tratamiento.

Párrafo 4 - Datos sensibles

235. El párrafo 4 se refiere a las medidas que las Partes deben adoptar en virtud del Protocolo al tratar determinados tipos de datos que puedan ser necesarios, en particular, como pruebas en una investigación o procedimiento penal, pero que, al mismo tiempo, sean de tal naturaleza que requieran salvaguardias adecuadas para evitar el riesgo de efectos perjudiciales injustificados para la persona afectada por la utilización de esos datos, en particular para prevenir la discriminación ilegal.

236. El párrafo 4 establece que los datos sensibles incluyen "los datos personales que revelen el origen racial o étnico; las opiniones políticas; las creencias religiosas o de otro tipo; la afiliación sindical; los datos genéticos; los datos biométricos considerados sensibles en vista de los riesgos que entrañan; o los datos personales relativos a la salud o a la vida sexual", que incluyen tanto la orientación sexual como las prácticas sexuales. Los datos sobre la salud pueden incluir datos que guardan relación con la salud física o mental de una persona que revelen información sobre su estado de salud pasado, presente o futuro (por ejemplo, información sobre una enfermedad, una discapacidad, un riesgo de enfermedad, el historial médico o el tratamiento de una persona, o el estado fisiológico o biomédico de la persona). Los datos genéticos pueden incluir, por ejemplo, los datos resultantes de análisis cromosómicos, de ADN o de ARN y los relacionados con las características genéticas heredadas o adquiridas de una persona que contengan información particular sobre su fisiología, salud o filiación.

237. El concepto de datos biométricos abarca una serie de identificadores particulares que corresponden a características físicas o fisiológicas mensurables utilizadas para identificar o verificar la supuesta identidad de una persona (por ejemplo, huellas dactilares, patrones del iris o de las venas de la palma de la mano, patrones de voz, fotografías o gra // opritbaciones de vídeo). Algunas Partes también consideran que los identificadores particulares que son fruto de características biológicas o de comportamiento constituyen datos biométricos. Si bien ciertas formas de datos biométricos pueden considerarse sensibles en vista de los riesgos que entrañan, otras formas pueden no serlo. Por ejemplo, algunas Partes consideran sensibles los datos biométricos calculados o extraídos de una muestra o imagen biométrica (como las plantillas biométricas).

En cambio, por lo general se consideraría que ciertas fotografías o vídeos, incluso si revelan rasgos físicos o anatómicos como cicatrices, marcas en la piel y tatuajes, no están comprendidos en la categoría de datos biométricos sensibles. Dado que el nivel de sensibilidad de los datos biométricos puede variar, el párrafo 4 concede a las Partes flexibilidad para regular este tema, al indicar que los datos sensibles incluyen "los datos biométricos considerados sensibles en vista de los riesgos que entrañan". Esa formulación reconoce que la biometría es un campo en evolución y que los datos considerados "sensibles" en virtud de este párrafo, los avances tecnológicos, de investigación y de otro tipo, y los riesgos para la persona implicada deberán ser evaluados a medida que avanza el tiempo. En lo que se refiere a las Partes en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), modificado por el Protocolo STCE nº 223, la interpretación de lo que constituye datos biométricos "sensibles" deberá guiarse por el artículo 6, párrafo 1, de dicho Convenio, tal como se expone en mayor detalle en los párrafos 58 y 59 del Informe explicativo de dicho Convenio.

238. La utilización y el tratamiento indebidos de datos sensibles plantea la posibilidad de riesgos de perjuicio injustificado para las personas, incluidos los riesgos de discriminación ilegal. El sistema de justicia penal debería estar configurado de manera que se puedan evitar consecuencias perjudiciales injustificadas y la discriminación ilegal basada, por ejemplo, en la utilización de pruebas que pongan de manifiesto la raza, la religión o la vida sexual. Como ejemplo adicional, este párrafo también reconoce la importancia de brindar protección contra el riesgo de daños que obedezcan a la revelación injustificada o ilegal de información, por ejemplo, que ocasione que una persona sea condenada al ostracismo por información que deje ver su orientación sexual o su identidad de género. A este respecto, el párrafo 4 exige a las Partes que establezcan "salvaguardias adecuadas" que brinden protección contra tales riesgos.

239. La idoneidad de las salvaguardias deberá evaluarse en función de la sensibilidad de los datos y del alcance, el contexto, los fines y la naturaleza del tratamiento (por ejemplo, en el caso de la toma de decisiones automatizada), así como de la probabilidad y la gravedad de los riesgos. Esas salvaguardias pueden variar de un ordenamiento jurídico a otro y depender de esos factores. Una lista no exhaustiva de salvaguardias puede incluir la restricción del tratamiento (por ejemplo, permitir el tratamiento de la información sólo para determinados fines o caso por caso); la restricción de la difusión; la restricción del acceso (por ejemplo, restringir el acceso sólo a determinado personal mediante procedimientos especiales de autorización o autenticación, que exigen una

formación especializada para dicho personal); las medidas adicionales de seguridad de índole organizativa o técnica (por ejemplo, enmascaramiento, seudonimización o almacenamiento por separado de los datos biométricos y de la información biográfica conexa), o los períodos de conservación más cortos. En algunos casos, puede ser útil realizar una evaluación del impacto para ayudar a identificar y gestionar los riesgos.

Párrafo 5 - Períodos de conservación

240. La primera frase del párrafo 5 establece que "[c]ada una de las Partes conservará los datos personales solo durante el tiempo que sea necesario y procedente para los fines del tratamiento de los datos de conformidad con el párrafo 2". A este respecto, el principio de restricción de la finalidad del párrafo 2 establece que una Parte que haya recibido datos personales procederá a su tratamiento para fines específicos de conformidad con el artículo 2 y que los datos no serán sometidos a un tratamiento posterior para un fin incompatible. En consonancia con dicho principio, el período de conservación de los datos está vinculado a la finalidad o finalidades específicas del tratamiento de los datos.

241. Puesto que, de conformidad con el artículo 2, los datos personales recibidos por una Parte con arreglo al presente Protocolo se facilitan para fines de investigaciones o procedimientos penales específicos, los datos personales podrán conservarse todo el tiempo que sea necesario: i) mientras dure la investigación y el procedimiento consiguiente, incluidos los recursos o períodos durante los cuales se pueda reabrir un caso con arreglo a la legislación nacional; y ii) una vez alcanzada la finalidad original de los datos recibidos, para su posterior tratamiento con un fin que "no sea incompatible" con la finalidad original. Por ejemplo, una Parte podrá disponer que la información o las pruebas se conserven con fines de archivo o de investigación histórica, u otros fines compatibles, acorde con el artículo 14, párrafo 2, como se explica en mayor detalle en los párrafos correspondientes del presente Informe explicativo.

242. La segunda frase del párrafo 5 ofrece a las Partes dos opciones para cumplir con la obligación de conservar los datos personales sólo durante el tiempo que sea necesario y procedente para los fines del tratamiento de los datos de conformidad con el párrafo 2 del presente artículo. En primer lugar, una Parte podrá establecer en su marco jurídico interno períodos de conservación específicos. Alternativamente, las Partes pueden prever en su marco jurídico interno la revisión a intervalos periódicos de la necesidad de ampliar la conservación. Las Partes tienen un margen de discreción para decidir qué

criterio, con arreglo a su marco jurídico interno, es el más apropiado para el conjunto específico de datos. Asimismo, las Partes podrán combinar un periodo de conservación específico con un sistema de revisiones periódicas a intervalos más cortos. Deberán garantizar en su marco jurídico que las autoridades competentes elaboren normas y/o procedimientos internos para aplicar los periodos de conservación específicos y/o la revisión periódica de la necesidad de un período de conservación adicional. Si el periodo de conservación ha expirado o si la Parte ha determinado, mediante una revisión periódica, que ya no es necesario conservar los datos, éstos deberán suprimirse o hacerse anónimos.

Párrafo 6 - Decisiones automatizadas

243. El párrafo 6 se refiere a la protección de las personas cuando las decisiones que produzcan un efecto negativo significativo en relación con los intereses pertinentes de la persona estén basadas únicamente en el tratamiento automatizado de sus datos personales. Cuando una Parte reciba datos personales de otra Parte en virtud del Protocolo, no se anticipan muchos casos de toma de decisiones automatizadas ya que las pruebas o la información serán obtenidas por los investigadores o las autoridades judiciales a efectos de una investigación o procedimiento penal específico. No obstante, si en la investigación para la que se solicitaron datos hubiera una toma de decisiones automatizadas que tuviera un efecto negativo significativo en relación con los intereses pertinentes de la persona a la que se refieren los datos personales, las autoridades deberán atenerse a esta disposición. Asimismo, las autoridades deben cumplir esta disposición si los datos son utilizados más tarde para la prevención, la detección, la investigación o el enjuiciamiento de otros delitos (por ejemplo, detención basada en el tratamiento puramente automatizado de perfiles delictivos, sentencias, libertad bajo fianza o libertad condicional), o para un fin compatible (por ejemplo, en el contexto de la verificación de antecedentes), si los datos están sujetos a herramientas analíticas automatizadas para fines de toma de decisiones.

244. Por lo tanto, el párrafo 6 prohíbe las decisiones basadas únicamente en el tratamiento automatizado de los datos personales cuando dicho tratamiento produzca un efecto negativo significativo en relación con los intereses pertinentes de la persona, incluidos los efectos jurídicos adversos (al afectar a la situación jurídica o a los derechos de la persona), como la emisión de una orden de detención o la denegación de la libertad bajo fianza o libertad condicional, a menos que dicha decisión esté autorizada por la legislación nacional y esté sujeta a las garantías adecuadas.

245. Las salvaguardias adecuadas son fundamentales para reducir el posible impacto sobre los intereses pertinentes de la persona a la que se refieren los datos personales. Dichas salvaguardias deben incluir la posibilidad de que la persona afectada pueda obtener intervención humana para evaluar la decisión. También se alienta a las Partes a que adopten medidas razonables destinadas a garantizar la calidad y representatividad de los datos utilizados en la elaboración de los algoritmos y la exactitud de las inferencias estadísticas utilizadas, teniendo en cuenta las circunstancias específicas y el contexto del tratamiento, incluido el contexto de la aplicación de la ley penal.

Párrafo 7 - Seguridad de los datos e incidentes de seguridad

246. De conformidad con el párrafo 7.a, "cada Parte garantizará que dispone de medidas tecnológicas, físicas y organizativas adecuadas para la protección de los datos personales". Por ejemplo, las medidas tecnológicas pueden incluir software de protección contra programas informáticos maliciosos, cifrado de datos y cortafuegos; las medidas físicas pueden incluir el almacenamiento de servidores y archivos informáticos en lugares seguros, y las medidas organizativas pueden incluir normas, prácticas, políticas y procedimientos, incluidos los que restringen los derechos de acceso.

247. El párrafo 7.a establece además que las medidas deben brindar protección, en particular, contra la pérdida (por ejemplo, procedimientos estandarizados para el archivado y tratamiento de los datos); el acceso accidental o no autorizado (por ejemplo, protecciones contra intrusiones informáticas, requisitos de autorización o autenticación para acceder a archivos en papel o informáticos); la divulgación accidental o no autorizada (por ejemplo, medidas tecnológicas para detectar y prevenir la divulgación accidental o no autorizada, y medidas organizativas para señalar las consecuencias de dicha divulgación); la alteración o destrucción accidental o no autorizada de datos (por ejemplo, restricción de la introducción o alteración de datos electrónicos o de archivos en papel al personal autorizado; la utilización de sistemas de registro automatizado de actividades, y la comunicación de los períodos de conservación; asimismo, deberán prever la instalación de sistemas de copia de seguridad de los archivos informáticos o en papel).

248. La forma concreta de cumplir esos requisitos de manera adecuada en circunstancias específicas es potestad de la Parte interesada. Se alienta a las Partes, por ejemplo, a que diseñen y apliquen medidas de seguridad que tomen en cuenta factores tales como la naturaleza de los datos personales (incluida su sensibilidad), los riesgos descubiertos y toda posible consecuencia adversa para la persona afectada en caso de un incidente de

seguridad. Al mismo tiempo, las Partes podrán tener en cuenta cuestiones relativas a los recursos necesarios para diseñar y aplicar las medidas de seguridad de los datos. Se alienta a las Partes a que sometan esas medidas a un examen periódico y a que las actualicen, cuando proceda, habida cuenta de la evolución de la tecnología y de la naturaleza cambiante de los riesgos.

249. El párrafo 7.b establece los requisitos en caso de que se descubra un "incidente de seguridad" (tal y como se define en el párrafo 7.a y se ha descrito *supra*) con respecto a los datos personales recibidos en virtud del Protocolo que den lugar a un "riesgo significativo de daño físico o no físico" para las personas o para la Parte de la que proceden los datos. El daño importante para las personas puede incluir, por ejemplo: daños corporales o a la reputación; angustia emocional (por ejemplo, debido a humillación, o una violación de la confidencialidad) y discriminación o daño económico (por ejemplo, pérdida de empleo o de oportunidades profesionales, calificación crediticia negativa, robo de identidad o posibilidad de chantaje). Por lo que respecta a la otra Parte, el daño importante puede incluir, en particular, las posibles repercusiones negativas en una investigación paralela (por ejemplo, fuga del sospechoso, destrucción de pruebas). Si existe un "riesgo significativo" de tal tipo de daño, la Parte receptora "evaluará sin demora la probabilidad y la magnitud del mismo y adoptará sin demora las medidas apropiadas para mitigar dicho daño". Los factores relativos a la probabilidad y la magnitud del daño que deben tenerse en cuenta pueden incluir, entre otros: el tipo de incidente y, si se conociera, si fue malicioso; las personas que tienen o podrían obtener la información; la naturaleza y sensibilidad de los datos afectados; el volumen de datos potencialmente comprometidos y el número de personas que pudieran verse afectadas; la facilidad de identificación de la persona o personas afectadas; la probabilidad de acceso y la utilización de los datos, por ejemplo, si los datos estaban cifrados o se habían empleado otros modos para hacerlos inaccesibles; y las posibles consecuencias que pudieran derivarse del incidente.

250. De acuerdo con las medidas expuestas en el párrafo 7.a, y con el fin de garantizar una respuesta adecuada en virtud del párrafo 7.b, las Partes deberán contar con procesos internos que permitan detectar incidentes de seguridad. También deberán tener un proceso que permita la rápida evaluación de la probabilidad y magnitud del posible daño, y la rápida adopción de medidas apropiadas para su mitigación (por ejemplo, retirando o solicitando la supresión de la información transmitida accidentalmente a un destinatario no autorizado). La aplicación eficaz de esos requisitos podría potenciarse con

los procedimientos internos de notificación y el mantenimiento de registros de todo incidente de seguridad.

251. El párrafo 7.b también presenta las circunstancias en las que se debe notificar el incidente a la otra Parte y a la(s) persona(s) afectada(s), sujeto a excepciones y restricciones.

252. En el caso de un incidente de seguridad en el que exista un riesgo significativo de daño físico o no físico para las personas o para la otra Parte, se enviará notificación también a la autoridad transferente o, a los efectos del capítulo II, sección 2, a la autoridad o autoridades designadas de conformidad con el Párrafo 7.c. No obstante, la notificación podrá incluir las correspondientes restricciones en cuanto a la transmisión ulterior de la notificación; asimismo, podrá retrasarse u omitirse cuando dicha notificación pueda poner en peligro la seguridad nacional, o retrasarse cuando dicha notificación pueda poner en peligro las medidas de protección de la seguridad pública (incluso cuando la notificación ponga en peligro la investigación de delitos penales derivados del incidente de seguridad). Al decidir si una notificación deberá retrasarse u omitirse en circunstancias en las que la notificación pueda poner en peligro la seguridad nacional, una Parte debe considerar si dadas las circunstancias sería razonable omitir la notificación o si, en cambio, sería más apropiado aplazarla.

253. En el caso de un incidente de seguridad que lleve aparejado un riesgo significativo de daño físico o no físico para las personas, se notificará también a la persona o personas afectadas por el incidente, con el fin de permitirles proteger sus intereses, aunque ello está sujeto a excepciones. En primer lugar, el párrafo 7.b establece que la notificación no es necesaria si la Parte ha tomado las medidas adecuadas para que ya no exista un riesgo significativo de daño. Por ejemplo, no será necesaria notificación cuando un correo electrónico que contenga información personal sensible haya sido enviado accidentalmente a un destinatario equivocado, lo que habría creado un riesgo significativo de daño sin medidas de mitigación, pero el correo fue eliminado rápida y permanentemente por el destinatario atendiendo a una petición antes de dar a conocer su contenido a terceros. En segundo lugar, la notificación a la persona podrá retrasarse u omitirse en las condiciones establecidas en el párrafo 12.a.i - es decir, la notificación "puede estar sujeta a la aplicación de restricciones proporcionadas permitidas en virtud de su marco jurídico interno, necesarias... para proteger los derechos y las libertades de otras personas u objetivos importantes de interés público general y que tengan debidamente en cuenta los intereses legítimos de la persona afectada."

254. De manera general, se alienta a las Partes a que, cuando proceda, incluyan en las notificaciones previstas en el párrafo 7.b información sobre el tipo de incidente de seguridad; el tipo y volumen de la información que puede haberse visto comprometida; los posibles riesgos, y las medidas que se prevé adoptar para mitigar los posibles daños, incluidas las medidas destinadas a contener el incidente. Habida cuenta de su función de supervisión, y con miras a beneficiarse del asesoramiento de expertos sobre la manera de mitigar el incidente, también podría resultar apropiado que la Parte que emite la notificación enviase información sobre el incidente y las medidas de mitigación a las autoridades de supervisión mencionadas en el párrafo 14.

255. Con el fin de facilitar una respuesta coordinada y brindar respaldo a sus propias medidas de mitigación del riesgo, la Parte notificada podrá solicitar de la Parte que envía la notificación consultas e información adicional sobre el incidente y la respuesta al mismo.

256. El párrafo 7.c establece los procedimientos necesarios para que las Partes designen a la autoridad o autoridades que deben ser notificadas de conformidad con el párrafo 7.b a efectos del capítulo II, sección 2.

Párrafo 8 - Mantenimiento de registros

257. El párrafo 8 exige que "cada Parte mantendrá registros o dispondrá de otros medios apropiados para demostrar cómo se accede, utiliza y divulga los datos personales de una persona en un caso concreto". Esto tiene como objeto que cada Parte disponga de medios eficaces para demostrar la manera en que se ha accedido, utilizado y divulgado en un caso concreto los datos de una persona específica, de acuerdo con el presente artículo. El poder demostrar el acatamiento de las disposiciones reviste importancia, en particular, a los efectos de la supervisión, y como tal contribuye a la rendición de cuentas. Aunque los medios precisos para demostrar la manera en que los datos han sido tratados se dejan a la discreción de cada una de las Partes, se las alienta a que adapten sus métodos a las circunstancias, teniendo en cuenta los riesgos para las personas afectadas y la naturaleza, el alcance, los fines y el contexto general del tratamiento de la información.

258. Por ejemplo, algunas Partes pueden decidir utilizar un registro automatizado de actividades (*logging*) u otras alternativas (como los registros manuscritos en el caso de los archivos en papel). Como se ha señalado anteriormente, la finalidad es facilitar la rendición de cuentas, pero concediendo cierto grado de flexibilidad en cuanto a la manera que adopte una Parte, en consonancia con otras obligaciones aplicables en virtud del artículo 14.

Por ejemplo, las Partes deberán mantener registros u otra documentación sobre el acceso, la utilización o la divulgación de manera que se facilite la labor de las autoridades de supervisión.

Párrafo 9 - Intercambio ulterior de información dentro de una Parte

259. El párrafo 9 establece que "[c]uando una autoridad de una Parte proporcione los datos personales recibidos inicialmente en virtud del presente Protocolo a otra autoridad de esa Parte, esa otra autoridad procederá a su tratamiento de conformidad con el presente artículo, sin perjuicio de lo dispuesto en el párrafo 9.b". En otras palabras, cuando los datos personales recibidos en virtud del Protocolo se faciliten posteriormente a otra autoridad de la misma Parte - incluso a una autoridad de un Estado constituyente u otra entidad territorial similar -, dichos datos deberán ser tratados de conformidad con el presente artículo, salvo que se aplique la excepción prevista en el párrafo 9.b. El párrafo 9 también se aplica en el caso de que se produzcan múltiples casos de intercambio posterior.

260. El párrafo 9.b establece una excepción al párrafo 9.a cuando una Parte que sea un Estado federal haya formulado una reserva a las obligaciones previstas en el artículo 17 del Protocolo, de conformidad con las condiciones establecidas en el mismo. En consonancia con el párrafo 297 del presente Informe explicativo, esta excepción tiene en cuenta "las dificultades que los Estados federales pueden enfrentar como resultado de la distribución de poderes entre las autoridades centrales y regionales". Esto es similar a lo dispuesto en el párrafo 316 del Informe explicativo del Convenio. Por lo tanto, el párrafo 9.b establece que, cuando una Parte haya formulado una reserva en virtud del artículo 17, podrá seguir facilitando los datos personales recibidos inicialmente en virtud del Protocolo a sus Estados constituyentes o a entidades territoriales similares, siempre que la Parte haya adoptado medidas para que las autoridades receptoras sigan protegiendo eficazmente los datos, al proporcionar un nivel de protección de los mismos comparable al que ofrece el presente artículo. El hecho de que una Parte no haya adoptado "medidas para que las autoridades receptoras sigan protegiendo eficazmente los datos, al proporcionar un nivel de protección de los datos comparable al que ofrece el presente artículo" puede, dependiendo de la gravedad, los motivos y las circunstancias del incumplimiento de este requisito, constituir una infracción material o sistemática en virtud del párrafo 15 del artículo 14.

261. El párrafo 9.c establece que en caso de que haya indicios de una aplicación indebida de este párrafo por otra Parte, la Parte de la que proceden los datos

podrá solicitar consultas y la información pertinente sobre esos indicios con el fin de aclarar la situación.

Párrafo 10 - Transferencia ulterior a otro Estado u organización internacional

262. De conformidad con el párrafo 10.a, una Parte podrá transferir los datos personales recibidos en virtud del Protocolo "a otro Estado u organización internacional únicamente con la autorización previa de la autoridad transferente o, a efectos del capítulo II, sección 2, de la autoridad o autoridades descritas en el párrafo 10.b". Este tipo de medida de protección es una condición común aplicada a las transferencias destinada a ayudar a las contrapartes extranjeras en el contexto de la aplicación de la ley penal (por ejemplo, en virtud de tratados de asistencia mutua o de cooperación entre cuerpos de policía), y ese criterio se integra en este párrafo también como medio de proteger los datos personales que se transfieran en virtud del Protocolo.

263. El párrafo 10.b establece que cada Parte, en el momento de la firma del presente Protocolo, o al depositar su instrumento de ratificación, aceptación o aprobación, comunicará al Secretario General del Consejo de Europa la autoridad o autoridades designadas para conceder la autorización en virtud del párrafo 10.a, a los efectos de las transferencias previstas en el capítulo II, sección 2, que podrá modificarse posteriormente.

264. La obtención de la autorización para una transferencia ulterior puede implicar que las autoridades de la Parte receptora envíen una solicitud individualizada a las autoridades de la Parte transferente para que se autorice la transferencia de datos personales indicados específicamente a un tercer país u organización internacional concretos. Sin embargo, el párrafo 10.a no impide que las Partes prescriban previamente reglas para las transferencias ulteriores (por ejemplo, mediante un acuerdo escrito u otras modalidades). El párrafo 10.a también se entiende sin perjuicio de la capacidad de una Parte para imponer otras condiciones a la utilización de los datos por la Parte receptora (por ejemplo, establecer restricciones a la latitud que la Parte receptora puede tener para utilizar o difundir los datos personales para evitar menoscabar la investigación de la Parte transferente) de conformidad con las disposiciones específicas del capítulo II.

265. A la hora de determinar si procede autorizar una transferencia en virtud del párrafo 10, se alienta a la autoridad transferente o designada a que tenga debidamente en cuenta todos los factores pertinentes, incluidos la gravedad de la infracción penal, la finalidad para la que se transfirieron originalmente los datos, toda condición aplicable relativa a la transferencia original, y si el tercer

país u organización internacional garantiza un nivel adecuado de protección de los datos personales.

Párrafo 11 - Transparencia y notificación

266. El párrafo 11.a impone a las Partes ciertos requisitos en materia de transparencia y notificación con respecto a los elementos especificados en los párrafos del 11.a.i al 11.a.iv. Estos requisitos de transparencia y notificación ayudan a las personas a entender la manera en que las Partes pueden proceder al tratamiento de sus datos. Estos requisitos también informan a las personas sobre el acceso, la rectificación y la reparación disponibles.

267. Cada Parte tiene flexibilidad para decidir si dicha notificación y transparencia ha de garantizarse mediante la publicación de avisos generales al público -por ejemplo, en un sitio web del gobierno - o mediante una notificación personal a la persona cuyos datos personales ha recibido la Parte. La notificación debe ser accesible sin dificultad y de fácil comprensión. Ya sea que se proporcione un aviso general o una notificación personal, deberá incluirse la siguiente información: i) la base jurídica para el tratamiento y su finalidad o finalidades, incluidos los fines de las divulgaciones anticipadas o habituales; ii) los períodos de conservación o revisión de conformidad con el párrafo 5 de este artículo, según corresponda; iii) los destinatarios o las categorías de destinatarios a los que se divulgan los datos y iv) el acceso, la rectificación y la reparación judicial y extra judicial disponibles.

268. En virtud del párrafo 11.b, cuando se notifique personalmente a la persona cuyos datos ha recibido la Parte, el requisito de notificación y transparencia del párrafo 11.a podrá estar sujeto a restricciones razonables de conformidad con las condiciones establecidas en el párrafo 12.a.i de este artículo. Por ejemplo, en lo que se refiere a las cuestiones de justicia penal puede haber circunstancias legítimas en las que se puede retrasar u omitir la notificación. Esas circunstancias se mencionan en el párrafo 12.a.i y se describen en el párrafo 272 del presente Informe explicativo. También pueden presentarse situaciones en las que podría restringirse la cantidad de detalles proporcionados en la notificación general, dependiendo de la sensibilidad de la información.

269. El párrafo 11.c proporciona una base para que las Partes sopesen el interés en la transparencia con la necesidad de confidencialidad en asuntos de justicia penal. Establece que cuando el marco jurídico nacional de la Parte transferente exija dar aviso personal a la persona cuyos datos han sido facilitados a otra Parte en virtud del Protocolo, la Parte transferente adoptará medidas para que la Parte receptora sea informada en el momento de la transferencia

con respecto a este requisito y reciba la información de contacto adecuada. La Parte transferente no notificará a la persona si la Parte receptora ha solicitado, cuando se apliquen las condiciones de restricción establecidas en el párrafo 12.a.i, que la provisión de los datos se mantenga confidencial. Una vez que dejen de aplicarse esas restricciones y se pueda proporcionar la notificación personal, la Parte receptora tomará medidas para que la Parte transferente sea informada de que puede procederse a la notificación. Ello puede incluir un examen periódico de la necesidad de tales restricciones. Si aún no ha sido informada, la Parte transferente tiene derecho a presentar solicitudes a la Parte receptora, la que informará a la Parte transferente si mantiene la restricción.

Párrafo 12 - Acceso y rectificación

270. El párrafo 12.a exige que cada Parte garantice que toda persona cuyos datos personales se hayan recibido en virtud del presente Protocolo tenga derecho a solicitar y obtener, de conformidad con los procedimientos establecidos en su ordenamiento jurídico interno y sin demora injustificada, el acceso a dichos datos (con sujeción a posibles restricciones) y, cuando esos datos sean inexactos o hayan sido tratados incorrectamente, a su rectificación. La expresión "de conformidad con los procedimientos establecidos en su marco jurídico interno" permite flexibilidad en cuanto a la forma en que las Partes pueden solicitar y obtener el acceso y la rectificación, y tiene por objeto aludir a los procedimientos establecidos, por ejemplo, en las leyes, reglamentos, normas (como las normas jurisdiccionales) y políticas aplicables, así como en las normas sobre las pruebas. En algunos ordenamientos jurídicos, una persona tendrá que solicitar el acceso y la rectificación por vía administrativa antes de sustanciar vías de recursos judiciales.

271. El párrafo 12.a.i establece que, en el caso de una solicitud de acceso, una persona tiene derecho a obtener una copia escrita o electrónica de la documentación que contenga sus datos personales y la información disponible que indique la base jurídica y los fines del tratamiento, la conservación y los destinatarios o las categorías de destinatarios de los datos ("acceso"), así como información relativa a las opciones disponibles para obtener reparación de conformidad con el párrafo 13. Esto también puede permitir a la persona confirmar si se han recibido (o no) sus datos personales con arreglo al Protocolo, y si ya han sido tratados o están siendo tratados. La entrega de documentación que contenga la información disponible que indique la base jurídica y los fines del tratamiento ayudará a la persona a evaluar si los datos personales están siendo tratados de conformidad con la legislación aplicable. Es posible que en muchas Partes ya exista un marco que permite otorgar ese

acceso con arreglo a sus leyes de privacidad, libertad de información o acceso a registros de la administración pública.

272. La capacidad de obtener dicho acceso a la información en un caso concreto puede estar sujeta a restricciones proporcionadas que son permitidas en virtud del marco jurídico interno de una Parte, "necesarias en el momento del fallo, para proteger los derechos y las libertades de otras personas u objetivos importantes de interés público general y que tengan debidamente en cuenta los intereses legítimos de la persona afectada". Los derechos y las libertades de otras personas pueden incluir, por ejemplo, la intimidad de otras personas cuyos datos personales serían dados a conocer en caso de que se conceda el acceso. Entre los objetivos importantes de interés público general pueden figurar, por ejemplo, la protección de la seguridad nacional y la seguridad pública (por ejemplo, la información sobre posibles amenazas terroristas o riesgos graves para los funcionarios encargados de hacer cumplir la ley); la prevención, la detección, la investigación o el enjuiciamiento de delitos penales; y la evitación de perjuicio a las indagaciones, investigaciones y procedimientos oficiales. De manera similar a la descripción de la proporcionalidad que figura en el párrafo 146 del Informe explicativo del Convenio, se espera que cada Parte aplique "restricciones proporcionadas" en este contexto, de conformidad con los principios pertinentes de su marco jurídico interno. En lo que se refiere a las Partes en el Convenio Europeo de Derechos Humanos (STE nº 5) o en el Protocolo STE nº 223 por el que se modifica el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, la proporcionalidad se entenderá con arreglo a lo dispuesto en dichos convenios. Otras Partes aplicarán principios conexos de su marco jurídico interno que limiten de manera razonable la capacidad de obtener acceso para proteger otros intereses legítimos. Como ya se ha señalado, las restricciones proporcionadas deberán proteger los derechos y libertades del prójimo o proteger objetivos importantes de interés público general y tomar debidamente en cuenta los "intereses legítimos de la persona afectada." En opinión de quienes participaron en la redacción, la expresión "intereses legítimos de la persona afectada" incluía los derechos y libertades de la persona. En caso de que se invoquen esos motivos de restricción, se insta a la autoridad requerida a que documente dicha decisión a efectos del párrafo 14. Las Partes también deberían considerar si se puede conceder acceso parcial cuando los motivos de cualquier restricción (por ejemplo, la protección de información comercial clasificada o confidencial) se apliquen solamente a determinadas partes de la información.

273. Cuando otras disposiciones del presente artículo permitan restricciones con arreglo a las condiciones establecidas en el párrafo 12.a.i, "en el momento del fallo" se refiere, en el caso del párrafo 7, al momento de la notificación de un incidente de seguridad; en el caso del párrafo 11.b, al momento de la notificación personal; y en el caso del 11.c, al momento en que una Parte solicita confidencialidad.

274. De acuerdo con el párrafo 12.a.ii., cada una de las Partes deberá velar por que una persona, cuyos datos hayan sido recibidos con arreglo a este Protocolo, tiene derecho a solicitar y obtener, de acuerdo con los procesos establecidos en su marco jurídico nacional y sin demora injustificada, la rectificación cuando los datos personales de la persona sean inexactos o hayan sido tratados incorrectamente. La rectificación incluirá -según corresponda y sea razonable teniendo en cuenta los motivos de la rectificación y el contexto particular del tratamiento- la corrección, la complementación (por ejemplo, mediante el marcado o el suministro de información adicional o correctiva), la supresión o la anonimización, la restricción del tratamiento o el bloqueo. A este respecto, quienes participaron en la redacción estimaron que la supresión o la anonimización es el curso de acción apropiado y razonable si los datos han sido tratados en violación del párrafo 5. En el caso de una violación del párrafo 2, también puede ser apropiado que la Parte restrinja el tratamiento; sin embargo, ello dependerá en última instancia del contexto particular (por ejemplo, la necesidad de mantener los datos personales con fines probatorios). Cuando se proceda a la anonimización de los datos, las Partes deberán evaluar el riesgo de una nueva identificación no autorizada y aplicar las medidas adecuadas para minimizar ese riesgo. Se alienta a las Partes a que, cuando sea factible, notifiquen toda medida de rectificación que se haya adoptado a la Parte de la que se recibieron los datos y a otras entidades con las que se hayan compartido los datos.

275. De acuerdo con el párrafo 12.b, si se deniega o restringe el acceso o la rectificación previstos en el párrafo 12.a, la Parte proporcionará a la persona, por escrito, que podrá ser por vía electrónica, sin demora injustificada, una respuesta en la que se le informe de la denegación o restricción. Si bien la autoridad deberá exponer los motivos de esa denegación o restricción, la comunicación podrá ser de carácter general (es decir, sin confirmar ni negar la existencia de ningún registro pertinente) cuando sea necesario para no socavar uno de los objetivos previstos en el párrafo 12.a.i. No obstante, las Partes se asegurarán de que la comunicación incluya información sobre las opciones de reparación disponibles.

276. Las Partes pueden cobrar una tasa para obtener el acceso (por ejemplo, el coste administrativo de la compilación y examen de los documentos a los que se ha solicitado acceso). Sin embargo, para no disuadir o desalentar el acceso, la tasa aplicada debe limitarse a lo que sea razonable y no excesivo dados los recursos que entraña. A fin de facilitar el ejercicio de los derechos establecidos en el párrafo 12.a se alienta a las Partes a que permitan a las personas pedir la ayuda de un representante para que solicite y obtenga las medidas descritas en ese párrafo, o para que presente una solicitud y/o reclamación en su nombre. En tales circunstancias, la notificación realizada de conformidad con el párrafo 11.a, así como la información obtenida en respuesta a una solicitud de acceso con arreglo al párrafo 12.a.i., pueden hacer referencia a esa posibilidad. Sin embargo, dicha representación deberá atenerse a los requisitos legales internos aplicables de la Parte en la que se solicitan tales medidas, o en que se presenta la solicitud y/o reclamación tal y como se ha descrito anteriormente, incluidas las normas que rigen las condiciones en las cuales personas o entidades pueden representar los intereses legales de otros (por ejemplo, en algunos ordenamientos jurídicos internos, las normas que rigen el poder notarial).

Párrafo 13 - Recursos judiciales y extrajudiciales

277. El párrafo 13 establece que "[c]ada Parte dispondrá de recursos judiciales y no judiciales efectivos para ofrecer reparación por las violaciones del presente artículo". Cada una de las Partes determinará el tipo de recursos que corresponde a las violaciones de las disposiciones de este artículo, y no se requiere que cada tipo de recurso esté disponible para cada una de las violaciones de este artículo. Los recursos previstos deben ser eficaces para hacer frente a las violaciones de este artículo. Cuando proceda, las Partes podrán incluir la compensación como reparación para el daño físico o no físico que el demandante haya demostrado que se deriva de la violación.

Párrafo 14 - Supervisión

278. El párrafo 14 establece que "cada Parte dispondrá de una o varias autoridades públicas que ejerzan, por sí solas o de forma acumulativa, funciones y facultades de supervisión independientes y eficaces con respecto a las medidas establecidas en el presente artículo". La disposición brinda flexibilidad a las Partes en cuanto a la forma de aplicar ese precepto. Algunas Partes pueden crear autoridades especializadas en protección de datos, mientras que otras pueden optar por ejercer la supervisión de forma acumulativa a través de más de una autoridad, cuyas funciones pueden solaparse. Ello refleja las diferencias en las estructuras constitucionales, organizativas y administrativas de las Partes.

En algunas Partes, esas autoridades de supervisión pueden pertenecer al componente de la administración pública cuyas actividades supervisan, y sus presupuestos pueden estar incluidos en el presupuesto general del componente. En tales casos, esas autoridades deben gozar de independencia para desempeñar eficazmente sus tareas de supervisión.

279. Quienes participaron en la redacción consideraron que varios elementos contribuyen a la independencia y eficacia de las funciones y competencias de supervisión. Las autoridades deben desempeñar sus funciones y ejercer sus facultades de manera imparcial; deben poder actuar libres de influencias externas que puedan interferir en el ejercicio independiente de sus facultades y funciones; en particular, dichas autoridades no deben estar sujetas a instrucciones, en un caso concreto, en cuanto al ejercicio de sus facultades de investigación y/o la adopción de medidas correctivas. Por último, es importante que las autoridades cuenten con las competencias, los conocimientos y la experiencia necesarios para desempeñar sus funciones, y que reciban los recursos financieros, técnicos y humanos adecuados para el desempeño eficaz de sus funciones.

280. Entre las funciones y facultades de esas autoridades "figurarán las facultades de investigación, de atender reclamaciones y de adoptar medidas correctivas". Quienes participaron en la redacción consideraron que las facultades de investigación deberían incluir el poder obtener la información necesaria para el desempeño de sus funciones, incluso, con sujeción a las condiciones pertinentes, el acceso a los registros mantenidos en virtud del párrafo 8. Las medidas correctivas pueden incluir: las advertencias en caso de incumplimiento; las instrucciones sobre la manera de lograr la conformidad de las operaciones de tratamiento de datos (por ejemplo, exigiendo la aplicación de medidas de seguridad adicionales destinadas a restringir el acceso a los datos o la rectificación de los datos personales); la exigencia de la suspensión (temporal) de determinadas operaciones de tratamiento, o la remisión del asunto a otras autoridades (por ejemplo, inspectores generales, fiscales, jueces de instrucción u órganos legislativos). Esas medidas correctivas podrán adoptarse por iniciativa propia de las autoridades o en respuesta a las reclamaciones presentadas por particulares en relación con el tratamiento de sus datos personales.

281. Se alienta a las Partes a que promuevan la cooperación entre sus respectivas autoridades de supervisión. Las autoridades de las Partes podrán celebrar consultas en el desempeño de sus funciones de supervisión establecidas en el presente artículo, según proceda. Ello puede incluir el intercambio de información y las mejores prácticas.

Párrafo 15 - Consulta y suspensión

282. El párrafo 15 determina cuándo, en virtud del artículo 14, una Parte podrá suspender la transferencia a otra Parte de datos personales con arreglo a lo dispuesto en el Protocolo cuando las Partes proceden de conformidad con el párrafo 1.a del artículo 14. En el párrafo 15 se aclara que, habida cuenta de los importantes fines coercitivos del presente Protocolo, dichas suspensiones deben producirse solamente en condiciones estrictas y con arreglo a los procedimientos específicos descritos en el mismo. Las disposiciones en materia de protección de datos contenidas en este artículo tienen por objeto proporcionar las salvaguardias adecuadas para la protección de los datos personales, incluso en caso de intercambio posterior dentro de una Parte y de transferencias ulteriores. Quienes participaron en la redacción consideraron que las salvaguardias recogidas en este artículo y su aplicación efectiva son esenciales y, por lo tanto, consideraron que era importante prever la suspensión de las transferencias de datos personales en situaciones concretas. Por consiguiente, una Parte podrá suspender la transferencia a otra Parte de datos personales en virtud del Protocolo si tiene pruebas sustanciales de que la otra Parte incumple sistemática o materialmente los términos del presente artículo, o de que es inminente un incumplimiento material. Si bien el requisito de las "pruebas sustanciales" no obliga a una Parte a demostrar un incumplimiento sistemático o material más allá de toda duda, tampoco permite suspender las transferencias basándose en una mera sospecha o conjetura. Más bien, la determinación de la Parte debe tener un apoyo sustancial en pruebas fácticas creíbles. Por "incumplimiento material" se entenderá una infracción significativa de una obligación material en virtud de este artículo. Ello puede incluir las limitaciones del marco jurídico de una Parte en cuanto a la obligación de aplicar salvaguardias que exige este artículo. Quienes participaron en la redacción reconocieron que la suspensión también se puede aplicar cuando existen infracciones sistemáticas, por ejemplo, infracciones recurrentes de las salvaguardias de este artículo. Quienes participaron en la redacción reconocieron además que la no aplicación de determinadas salvaguardias en relación con el tratamiento de los datos personales en un caso individual, en ausencia de un incumplimiento material, no constituirá motivo suficiente para invocar esta disposición, ya que la persona afectada debería poder hacer frente a esas infracciones mediante reparaciones adecuadas, tanto extrajudiciales como judiciales, con arreglo a lo previsto en el párrafo 13 del artículo 14.

283. El párrafo 15 establece además que una Parte "no suspenderá las transferencias sin previo aviso razonable, y no lo hará hasta después de que las

Partes afectadas hayan iniciado un periodo razonable de consultas sin llegar a una resolución". Este requisito de consulta reconoce que la suspensión de las transferencias esenciales para la aplicación de la ley sólo debe tener lugar después de conceder a la otra Parte una oportunidad razonable para que aclare la situación o atienda las preocupaciones declaradas. Al inicio de dicha consulta, la Parte que invoque este párrafo podrá solicitar a la otra Parte que le proporcione información pertinente. Sin embargo, como se reconoce en el párrafo 15, la Parte que invoque este párrafo debe disponer de antemano de pruebas sustanciales de un incumplimiento sistemático o material, o de que es inminente un incumplimiento material; por lo tanto, no deberá recurrirse al mecanismo de consulta para recabar más pruebas cuando sólo existan sospechas de una infracción. Las transferencias de datos en virtud del Protocolo sólo podrán suspenderse tras un preaviso razonable y un periodo razonable de consultas sin que se haya alcanzado una resolución. Sin embargo, una Parte podrá suspender provisionalmente las transferencias en el caso de una infracción sistemática o material que suponga un riesgo significativo e inminente para la vida o la seguridad de una persona física, o un daño sustancial a su reputación o su situación económica. Ello incluye un riesgo significativo e inminente de lesiones corporales o daño para la salud de una persona física. En esos casos, la Parte deberá notificarlo a la otra Parte e iniciar consultas con ella inmediatamente después de suspender provisionalmente las transferencias. Quienes participaron en la redacción consideraron que la suspensión provisional debería limitarse, en general, a las transferencias que guardan una relación directa con la exigencia que justifica la suspensión provisional.

284. Si la Parte que suspende cumple las condiciones establecidas en el párrafo 15, podrá suspender las transferencias y la otra Parte no podrá imponer una suspensión recíproca. Sin embargo, si la otra Parte tiene pruebas sustanciales de que la suspensión por la Parte que suspende es contraria a los términos del párrafo 15, podrá suspender recíprocamente las transferencias de datos a la Parte que suspende. En este contexto, el significado del término "pruebas sustanciales" es idéntico al que tiene en lo que respecta a la suspensión inicial por la Parte que la suspende. La suspensión por la Parte que suspende sería contraria a lo dispuesto en el párrafo 15 si, por ejemplo, la Parte que suspende no dispusiera de "pruebas sustanciales", si el incumplimiento no fuera "sistemático" ni "material", o si la Parte que suspende no hubiere cumplido los requisitos de procedimiento para la suspensión, en particular los relativos a las consultas.

285. Por último, el párrafo 15 establece que la "Parte que suspende levantará la suspensión tan pronto como se haya subsanado la infracción que justifica la suspensión" y que "cualquier suspensión recíproca se levantará en ese momento". En el contexto de la suspensión prevista en el presente párrafo se aplicará una norma similar a la que se aplica en el artículo 24, párrafo 4. Es decir, el párrafo 15 establece que "los datos personales transferidos antes de la suspensión seguirán siendo tratados de conformidad con el presente Protocolo."

286. Se alienta a las Partes a que hagan pública o notifiquen oficialmente cualquier suspensión o suspensión provisional en virtud de este párrafo a los proveedores de servicios y a las entidades que puedan recibir solicitudes u órdenes en virtud del capítulo II, sección 2. Dicha comunicación puede ser importante para suspender en la práctica las transferencias de datos personales a una Parte que incumpla material o sistemáticamente el presente artículo, y también para garantizar que los proveedores de servicios y las entidades no restrinjan la transferencia de información o pruebas en virtud del presente Protocolo basados en la creencia errónea de que una Parte está sujeta a esta disposición de suspensión.

287. Aunque el párrafo 15 establece procedimientos específicos relativos a las consultas y la suspensión de las transferencias de datos personales por motivos de protección de datos, los procedimientos del párrafo 15 no tienen por objeto afectar a las consultas previstas en el artículo 23, párrafo 1, ni a los derechos de suspensión que puedan ser aplicables en virtud del derecho internacional con respecto a otros artículos del presente Protocolo.

Capítulo IV - Disposiciones finales

288. Las disposiciones contenidas en este capítulo están basadas, en su mayor parte, en el "Modelo de cláusulas finales para los convenios, protocolos adicionales y protocolos modificativos concluidos en el seno del Consejo de Europa", que fue adoptado por el Comité de Ministros en la 1291ª reunión de los delegados de los ministros en julio de 2017, y también en las cláusulas finales del Convenio. Dado que algunos de los artículos de este capítulo utilizan las formulaciones estándar de las cláusulas modelo o se basan en la práctica habitual en materia de elaboración de tratados en el Consejo de Europa, no son necesarios comentarios específicos. Sin embargo, algunas modificaciones de las cláusulas modelo estándar y las diferencias respecto de las disposiciones finales del Convenio requieren alguna explicación.

Artículo 15 - Efectos del presente Protocolo

289. El párrafo 1.a del artículo 15 incorpora el artículo 39, párrafo 2, del Convenio. Como se reconoce en el párrafo 312 del Informe explicativo del Convenio, este párrafo establece que las Partes son libres de aplicar los acuerdos ya existentes o que puedan entrar en vigor en el futuro. Al igual que el Convenio, este Protocolo por lo general establece obligaciones mínimas; por lo tanto, en este párrafo se reconoce que las Partes son libres de asumir obligaciones más específicas, además de las ya establecidas en este Protocolo, a la hora de establecer sus relaciones en relación con los asuntos tratados en el mismo. Sin embargo, al hacerlo las Partes deben respetar los objetivos y principios del Protocolo y, por lo tanto, no pueden aceptar obligaciones que anulen la finalidad perseguida.

290. El párrafo 1.b de este artículo también reconoce la creciente integración de la Unión Europea (UE) desde que el Convenio se abrió a la firma en 2001, en particular en lo que respecta a la aplicación de la ley y la cooperación judicial en materia penal, así como a la protección de los datos. Por consiguiente, permite a los Estados miembros de la UE aplicar entre ellos el derecho de la Unión Europea que rige las cuestiones comprendidas en este Protocolo. En el criterio de quienes participaron en la redacción, el derecho de la Unión Europea incluye las medidas, los principios y los procedimientos previstos en el ordenamiento jurídico de la UE, en particular, las disposiciones legales, reglamentarias o administrativas, así como otros requisitos, incluidas las resoluciones judiciales. Por lo tanto, el párrafo 1.b tiene por objeto abarcar las relaciones internas entre los Estados miembros de la UE y entre los Estados miembros de la UE y las instituciones, órganos y organismos de la UE. Si no existe una legislación de la Unión Europea relativa a una cuestión comprendida en el ámbito de aplicación del presente Protocolo, el Protocolo seguirá rigiendo esa cuestión entre las Partes que sean Estados miembros de la UE.

291. El párrafo 1.c aclara que el párrafo 1.b no afecta a la plena aplicación del presente Protocolo entre las Partes que son miembros de la UE y las demás Partes. Por lo tanto, el párrafo 1.b no pretende tener ningún efecto que vaya más allá de las relaciones internas de la UE, tal y como se expone en el párrafo 290 *supra*; este Protocolo se aplica plenamente entre las Partes que son Estados miembros de la UE y otras Partes. Quienes participaron en la redacción consideraron que esa disposición era esencial para garantizar que las Partes que no son Estados miembros de la UE pudieran acogerse a todos los beneficios de este Protocolo en sus relaciones con las Partes que son Estados miembros de la UE. Por ejemplo, quienes participaron en la redacción consideraron que

un Estado miembro de la UE que reciba información o pruebas de una Parte que no pertenece a la UE tendría que solicitar el consentimiento de la Parte que no pertenece a la UE antes de transferir la información o las pruebas a otra Parte que es miembro de la UE, en consonancia con el artículo 14, párrafo 10. Del mismo modo, el párrafo 1.a de este artículo se aplicaría plenamente entre las Partes que son Estados miembros de la UE y otras Partes que no lo son.

292. El párrafo 2 de este artículo incorpora el artículo 39, párrafo 3, del Convenio. Al igual que el Convenio, como se explica en el párrafo 314 del Informe explicativo del Convenio, este Protocolo no pretende abordar todas las cuestiones pendientes que guardan relación con las formas de cooperación entre las Partes o entre las Partes y las entidades privadas en lo relativo a la ciberdelincuencia y la recopilación de pruebas en forma electrónica de los delitos penales. Por lo tanto, el párrafo 2 del artículo 15 se incluyó para dejar claro que el Protocolo sólo afecta a los aspectos abordados en el mismo. No se ven afectados otros derechos, restricciones, obligaciones y responsabilidades que puedan existir pero que no están contemplados en este Protocolo.

293. El artículo 15 no contiene una disposición análoga a la del artículo 39, párrafo 1, del Convenio. Esa disposición del Convenio explicaba que la finalidad del Convenio era completar los tratados o acuerdos bilaterales aplicables entre las Partes, incluidos ciertos tratados de extradición y asistencia mutua. Este Protocolo no contiene ninguna disposición en materia de extradición e incluye muchas disposiciones que no son disposiciones sobre asistencia mutua. Como se explica en mayor detalle en el artículo 5 y en el Informe explicativo concomitante, cada sección de las medidas de cooperación del capítulo II interactúa de diferentes maneras con los tratados de asistencia mutua. Por consiguiente, quienes participaron en la redacción llegaron a la conclusión de que no era necesario incluir una disposición similar a la que figura en el artículo 39, párrafo 1.

Artículo 16 - Firma y entrada en vigor

294. El artículo 16 permite que todas las Partes en el Convenio firmen y sean Partes en el presente Protocolo. A diferencia del Primer Protocolo (artículo 11), el presente Protocolo no prevé un procedimiento de adhesión a este Protocolo. Todo Estado que desee firmar y convertirse en Parte en este Protocolo deberá primero pasar a ser Parte en el Convenio.

295. El párrafo 3 establece que "el presente Protocolo entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses a partir

de la fecha en que cinco Partes en el Convenio hayan expresado su consentimiento para quedar vinculados por el presente Protocolo". Si bien el Convenio establecía en su artículo 36, párrafo 3, que al menos tres de las cinco Partes debían ser Estados miembros del Consejo de Europa para que el Convenio entrara en vigor, tal requisito no se incluye en el presente Protocolo, dado que se trata de un protocolo adicional a un Convenio y que todas las Partes deberían tener el mismo derecho a aplicarlo tan pronto como un número mínimo de cinco Partes en el Convenio hayan expresado su consentimiento en quedar obligadas. Esto concuerda con lo planteado en el artículo 10 del Primer Protocolo.

296. El párrafo 4 describe el proceso para la entrada en vigor del presente Protocolo para toda Parte en el Convenio que exprese su consentimiento en quedar vinculada por el presente Protocolo, tras su entrada en vigor de conformidad con el párrafo 3. Esto concuerda con lo planteado en el párrafo 4 del artículo 36 del Convenio.

Artículo 17 -Cláusula federal

297. Al igual que la cláusula federal que figura en el artículo 41 del Convenio, el artículo 17 del presente Protocolo incluye una cláusula federal que permite a una Parte que sea un Estado federal adoptar una reserva "compatible con los principios fundamentales que rigen las relaciones entre su gobierno central y los Estados constituyentes u otras entidades territoriales similares". La finalidad del artículo 17 es idéntica a la del artículo 41 del Convenio. Es decir, como se indica en el párrafo 316 del Informe explicativo del Convenio, "tiene como finalidad allanar las dificultades que los Estados federales pueden enfrentar como resultado de la distribución de poderes entre autoridades centrales y regionales."

298. Se permitió a los Estados federales formular una reserva a las obligaciones establecidas en el capítulo II del Convenio (establecimiento de delitos penales internos y medidas procesales internas), siempre que las medidas no sean competencia del gobierno central de un Estado federal. Sin embargo, los Estados federales deben poder prestar cooperación internacional a otras Partes en virtud del capítulo III del Convenio.

299. Aunque este Protocolo prevé la cooperación internacional en lugar de medidas nacionales, los negociadores reconocieron que sigue siendo necesario incluir una cláusula federal en el Protocolo. Mientras que el Convenio no preveía ninguna reserva para los Estados federales en materia de asistencia mutua, la mayoría de las medidas del Protocolo no se aplican de la misma

manera que la asistencia mutua tradicional. El Protocolo incluye una serie de medidas de cooperación que son más eficientes que la asistencia mutua tradicional y que no requieren necesariamente la participación del gobierno central. En particular, el Protocolo introduce dos medidas, reflejadas en los artículos 6 y 7, en virtud de las cuales las autoridades competentes de una Parte pueden solicitar directamente la cooperación de empresas privadas en otra Parte. Esas medidas requieren ciertos trámites procesales que podrían plantear dificultades a un Estado federal, que no puede exigir su cumplimiento a las autoridades competentes de los Estados o entidades territoriales constituyentes. Por ejemplo, el artículo 7 establece que una Parte podrá, mediante notificación al Secretario General, exigir que las autoridades de otras Partes notifiquen simultáneamente a una autoridad pública designada cuando transmitan a un proveedor de servicios una orden en que pidan información relativa al abonado. Otros artículos incluyen requisitos para la adopción de medidas legislativas o de otro tipo; sin embargo, un Estado federal podría no estar facultado para exigir a sus Estados constituyentes u otras entidades territoriales similares que promulgasen ese tipo de medidas. Por último, el Protocolo incluye disposiciones pormenorizadas en materia de protección de datos, que no existían en el Convenio. Por ejemplo, en los Estados Unidos, en virtud de su Constitución y de los principios fundamentales del federalismo, los Estados constituyentes promulgan sus propias leyes penales y de procedimiento penal (con independencia de las leyes federales); establecen sus propios tribunales, fiscales y policía, e investigan y persiguen los delitos penales cometidos en esos Estados. Las autoridades estatales competentes son independientes de las autoridades federales y no están subordinadas a ellas.

300. En caso de que las autoridades de un Estado constituyente de un Estado federal o entidad territorial similar solicitaran las formas de cooperación previstas en el Protocolo, podría ocurrir que: i) esas autoridades aplicasen leyes de procedimiento y de privacidad diferentes a las adoptadas por las autoridades del gobierno central; ii) no respondiesen al gobierno central en términos de jerarquía organizativa, o que iii) el gobierno central no tuviese la capacidad jurídica para orientar sus actuaciones. En tales situaciones, no existirían garantías de que un Estado constituyente o una entidad territorial similar habría de cumplir con los requisitos establecidos en el Protocolo – tanto los relativos a la obtención de información o pruebas como los referentes al tratamiento posterior de dicha información o pruebas – a menos que: i) fueran aplicadas por el Estado mismo, o ii) sus autoridades solicitaran la cooperación a través de las autoridades del gobierno central,

o con la participación de éstas, que velarían por el cumplimiento de lo previsto (por ejemplo, mediante asistencia mutua o a través del punto de contacto 24/7, o con la participación del gobierno central en un equipo conjunto de investigación).

301. Habida cuenta de esas cuestiones, el párrafo 1 dispone que las Partes que sean Estados federales podrán formular reservas. Esas Partes podrán reservarse el derecho de asumir las obligaciones en virtud del presente Protocolo que sean compatibles con los principios fundamentales que rigen las relaciones entre su gobierno central y los Estados constituyentes u otras entidades territoriales similares, sujeto a lo dispuesto en los párrafos del 1.a al 1.c, que restringen el ámbito de dicha reserva. En virtud del párrafo 1.a, el gobierno central de un Estado federal que invoque esta reserva está obligado a aplicar todas las disposiciones del Protocolo (sin perjuicio de las reservas y declaraciones disponibles). En lo referente a las obligaciones de protección de datos en virtud del Protocolo, por lo que se refiere a las Partes que procedan con arreglo al artículo 14, párrafo 1.a, ello incluye las obligaciones establecidas en el artículo 14, párrafo 9.b, en relación con el intercambio posterior de información con los Estados constituyentes u otras entidades territoriales similares (véase el párrafo 260 del Informe explicativo) cuando una autoridad federal haya solicitado información con arreglo al Protocolo para sus propios fines o en nombre de una autoridad a nivel subfederal y posteriormente comparta esa información con dicha autoridad a nivel subfederal. Asimismo, el párrafo 1.b establece que, de forma similar a lo dispuesto en el artículo 41, párrafo 1, del Convenio, dicha reserva no afectará a las obligaciones de ese Estado federal Parte para brindar la cooperación que soliciten otras Partes de conformidad con las disposiciones del capítulo II. Por último, en virtud del párrafo 1.c, no obstante la reserva formulada por un Estado federal, el artículo 13 del presente Protocolo -que exige, como dispone el artículo 15 del Convenio, la protección de los derechos humanos y las libertades en virtud del derecho interno- se aplica a los Estados constituyentes del Estado federal o a otras entidades territoriales similares, además del gobierno central en virtud del párrafo 1.a.

302. El párrafo 2 establece que si un Estado federal formula una reserva con arreglo al párrafo 1, y las autoridades de un Estado constituyente o entidad territorial similar de esa Parte solicitan directamente la cooperación de una autoridad, proveedor o entidad en otra Parte, esa otra Parte "podrá impedir que las autoridades, proveedores o entidades en su territorio cooperen en respuesta" a dicha solicitud. La otra Parte podrá determinar la manera de

impedir la cooperación de sus autoridades, proveedores o entidades en su territorio. Hay dos excepciones a la facultad de la otra Parte de impedir la cooperación:

303. En primer lugar, el párrafo 2 dispone que esa otra Parte no podrá impedir la cooperación si, cuando el Estado constituyente u otra entidad territorial similar acate las obligaciones del presente Protocolo, el Estado federal Parte interesado ha "notificado al Secretario General del Consejo de Europa que un Estado constituyente u otra entidad territorial similar aplica las obligaciones del presente Protocolo aplicables a dicho Estado federal". La expresión "obligaciones del presente Protocolo aplicables a dicho Estado federal" quiere decir que una autoridad de un Estado constituyente o entidad territorial similar no puede estar sujeta a ninguna obligación a la que no esté sujeto el gobierno central, como, por ej., una reserva aplicable. Si el Estado federal ha formulado esa notificación al Secretario General con respecto a un Estado constituyente concreto, la otra Parte está obligada a disponer la ejecución de una orden o solicitud emitida por ese Estado en la misma medida que si se hubiera recibido de las autoridades del gobierno central. Por supuesto, los requisitos y procedimientos incluidos en cada una de las medidas de cooperación del capítulo II siguen siendo aplicables a las solicitudes u órdenes presentadas por dichos Estados constituyentes o entidades territoriales similares; el cumplimiento de dichos requisitos es necesario. Este párrafo requiere que el Secretario General del Consejo de Europa establezca y mantenga actualizado un registro de dichas notificaciones. Se alienta a las partes a que proporcionen al Secretario General información actualizada.

304. En segundo lugar, en virtud del párrafo 3, si un Estado constituyente u otra entidad territorial similar ha presentado una solicitud u orden a través del gobierno central o, con arreglo al artículo 12, en virtud de un acuerdo de creación de un equipo conjunto de investigación celebrado con la participación del gobierno central, la otra Parte no podrá impedir que las autoridades, los proveedores o las entidades en su territorio transfieran información o pruebas con arreglo a lo dispuesto en el Protocolo aduciendo que la cooperación ha sido solicitada por un Estado constituyente o una entidad territorial similar de un Estado federal que ha adoptado la reserva prevista en el párrafo 1. Esto se debe a que cuando la solicitud o la orden ha sido presentada por conducto del gobierno central o del equipo conjunto de investigación establecido con la participación del Gobierno central, éste "velará por el cumplimiento de las obligaciones aplicables del Protocolo". Dado que el gobierno central es quien presenta la solicitud u orden (o participa en el equipo conjunto de

investigación), el gobierno central tiene la oportunidad y la obligación de verificar el cumplimiento de los requisitos del Protocolo en relación con esas medidas. Por ejemplo, si, en virtud del artículo 7, párrafo 5.a, es necesario notificar a otra Parte acerca de la transmisión de una orden destinada a obtener información relativa a los abonados, el gobierno central está obligado a hacer esa notificación. Con respecto a la protección de datos (tratándose de las Partes que proceden en virtud del Artículo 14, párrafo 1.a), si un Estado constituyente u otra entidad territorial similar solicita la cooperación a través del gobierno central, éste proporciona los datos al Estado constituyente u otra entidad territorial similar y debe aplicar lo dispuesto en el Artículo 14, párrafo 9.b (intercambio de información dentro de una Parte). Es decir, el gobierno central debe contar con medidas que permitan a las autoridades receptoras seguir brindando protección eficaz de los datos para lo cual establecerá un nivel de protección comparable al previsto en el artículo 14. Las autoridades de un Estado constituyente o de una entidad territorial similar que solicite y reciba datos personales de esta manera no están obligadas por lo demás a aplicar el artículo 14. Si las Partes interesadas aplican otro acuerdo o convenio especificado en el artículo 14, párrafos 1.b o 1.c, se aplicarán las "disposiciones de dicho acuerdo o convenio".

305. El texto del párrafo 4 es idéntico al del artículo 41, párrafo 3 del Convenio y tiene el mismo efecto. Por lo tanto, en lo que respecta a las disposiciones del Convenio cuya aplicación es competencia de los Estados constituyentes u otras entidades territoriales similares (a menos que se haya notificado al Secretario General del Consejo de Europa, de conformidad con lo dispuesto en el párrafo 2 del presente artículo), el gobierno central del Estado federal está obligado a: i) informar a las autoridades de sus Estados constituyentes u otras entidades territoriales similares acerca de las disposiciones del presente Protocolo; y ii) dar "su dictamen favorable, instándoles a adoptar las medidas adecuadas para ponerlas en práctica", lo que alienta a los Estados constituyentes o entidades territoriales similares a aplicar plenamente el Protocolo. En lo referente al Protocolo, ello también tiene por objeto permitir eventualmente que esos Estados constituyentes u otras entidades territoriales similares reciban la notificación prevista en el párrafo 2 del presente artículo.

Artículo 18 - Aplicación territorial

306. El artículo 38 del Convenio permite a las Partes especificar el territorio o territorios a los que se aplicará el Convenio. El artículo 18 del presente

Protocolo se aplicará automáticamente a los territorios especificados por una Parte en una declaración formulada en virtud del artículo 38, párrafo 1 o párrafo 2 del Convenio, en la medida en que dicha declaración no haya sido retirada conforme a lo dispuesto en el artículo 38, párrafo 3, del Convenio. Quienes participaron en la redacción consideraron que lo mejor sería que el Convenio y el presente Protocolo tuvieran el mismo ámbito territorial como norma por defecto.

307. El párrafo 2 de este artículo establece que "[una] Parte podrá, en el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, declarar que el presente Protocolo no se aplicará a uno o más territorios especificados en la declaración de la Parte en virtud de los párrafos 1 y/o 2 del artículo 38 del Convenio". De conformidad con el párrafo 3, las Partes podrán retirar la declaración que figura en el párrafo 2 del presente artículo, de conformidad con los procedimientos especificados. La retirada de la declaración que figura en el párrafo 2 tendría el efecto de aplicar el presente Protocolo a otros territorios comprendidos en el Convenio pero a los que el presente Protocolo no se había aplicado previamente.

308. Este artículo no permite aplicar el presente Protocolo a territorios no comprendidos en el Convenio.

Artículo 19 - Reservas y declaraciones

309. Este artículo prevé diversas posibilidades de reserva. Dado el alcance mundial del Convenio y el objetivo de lograr el mismo nivel de adhesión al presente Protocolo, dichas reservas permiten a las Partes en el Convenio pasar a ser Partes en el presente Protocolo, al tiempo que permiten a esas Partes mantener ciertos enfoques y conceptos coherentes con su derecho interno, sus principios jurídicos fundamentales o consideraciones de política, como corresponda.

310. Las posibilidades de formular reservas están limitadas a fin de garantizar en la mayor medida posible la aplicación uniforme del presente Protocolo por las Partes. Por lo tanto, no podrán formularse más reservas que las enumeradas. Además, las reservas sólo podrán ser formuladas por una Parte en el Convenio en el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación.

311. Al igual que en el Convenio, en el presente Protocolo las reservas excluyen o modifican los efectos jurídicos de las obligaciones incluidas en el presente Protocolo (véase el párrafo 315 del Informe explicativo del Convenio). En el

presente Protocolo, se permiten reservas para excluir en su conjunto algunas formas de cooperación. Concretamente, el artículo 7, párrafo 9.a, permite que una Parte pueda reservarse el derecho de no aplicar este artículo en su totalidad. Asimismo, se permiten reservas destinadas a excluir la cooperación en relación con artículos enteros en lo que respecta a determinados tipos de datos. En concreto, el artículo 7, párrafo 9.b, permite a una Parte reservarse el derecho de no aplicar el artículo 7 a determinados tipos de números de acceso si la divulgación de esos números de acceso fuera incompatible con los principios fundamentales de su ordenamiento jurídico interno. Del mismo modo, el artículo 8, párrafo 13, permite a una Parte reservarse el derecho de no aplicar el artículo 8 a los datos sobre el tráfico.

312. El artículo 19 también se refiere a las declaraciones. Al igual que en el Convenio, en el presente Protocolo se permite a las Partes formular declaraciones para incluir determinados procedimientos adicionales especificados que modifican el alcance de las disposiciones. Esos procedimientos adicionales tienen por objeto dar cabida a diferencias conceptuales, jurídicas o prácticas concretas, que se justifican en vista de la esfera de acción mundial del Convenio y la aspiración de que el presente Protocolo tenga una cobertura idéntica. Las declaraciones enumeradas se dividen en dos categorías generales:

313. Varias declaraciones permiten a una Parte declarar que ciertas facultades o medidas deberán corresponder a autoridades específicas, o que la cooperación debe transitar por determinados canales. Este es el caso del artículo 10, párrafo 9 (que permite declarar que las solicitudes también podrán ser enviadas directamente a otras autoridades además de la autoridad central); el artículo 12, párrafo 3 (la autoridad central deberá ser signataria del acuerdo por el que se establece el equipo conjunto de investigación o estar de otra manera de acuerdo con él); el artículo 8, párrafo 11 (una Parte declarante puede exigir que las solicitudes en virtud de este artículo formuladas por otras Partes le sean presentadas por la autoridad central de la Parte requirente u otra autoridad determinada de común acuerdo).

314. Una segunda categoría de declaraciones permite a las Partes exigir trámites de procedimiento distintos o adicionales en relación con medidas concretas o en materia de cooperación con el fin de cumplir con la legislación nacional o evitar sobrecargar a las autoridades. Por ejemplo, el artículo 7, párrafo 8, y el artículo 9, párrafo 1.b, permiten a una Parte hacer declaraciones para exigir que otras Partes adopten medidas de procedimiento concretas

con respecto a la información relativa al abonado. El Artículo 7, párrafos 2.b y 5.a; el Artículo 8, párrafo 4, y el Artículo 9, párrafo 5, permiten trámites de procedimiento adicionales para proporcionar salvaguardias adicionales o para acatar la legislación nacional. No está previsto que las declaraciones tengan efectos recíprocos. Por ejemplo, si una Parte hace una declaración en virtud del artículo 10, párrafo 9 – en el sentido de que las solicitudes en virtud de este artículo deberán dirigirse únicamente a su autoridad central - las demás Partes podrán dirigir las solicitudes a las autoridades adicionales de la Parte que ha hecho la declaración, pero ésta podrá solamente enviar solicitudes a las autoridades centrales de las demás Partes, a menos que éstas también hagan una declaración en ese sentido.

315. Las declaraciones mencionadas en el párrafo 2 del presente artículo deberán hacerse en el momento de la firma de una Parte o en el momento del depósito de su instrumento de ratificación, aceptación o aprobación. En cambio, las declaraciones que figuran en el párrafo 3 podrán hacerse en cualquier momento.

316. En el párrafo 3 se exige a las Partes que notifiquen al Secretario General del Consejo de Europa toda declaración, notificación o comunicación a que se hace referencia en el artículo 7, párrafos 5.a y 5e; en el artículo 8, párrafos 4 y 10.a y 10.b, en el artículo 14, párrafos 7.c y 10.b, y el artículo 17, párrafo 2 del presente Protocolo, conforme a los términos especificados en dichos artículos. Por ejemplo, en virtud del artículo 7, párrafo 5.e, "la Parte, en el momento de la primera notificación al Secretario General de conformidad con el párrafo 5.a deberá comunicar al Secretario General del Consejo de Europa la información de contacto de dicha autoridad". Además, las Partes comunicarán al Secretario General del Consejo de Europa las "autoridades" a las que se refiere el artículo 8, párrafos 10.a y 10.b. Se ha encargado al Secretario General que establezca y mantenga actualizado un registro de esas autoridades designadas por las Partes, y se ordena a las Partes que se aseguren de que los datos que proporcionan para el registro sean correctos en todo momento (véase el artículo 7, párrafo 5.f, y el artículo 8, párrafo 12).

Artículo 20 - Situación y retirada de las reservas

317. Al igual que el artículo 43 del Convenio, este artículo, sin imponer plazos específicos, exige a las Partes que retiren las reservas tan pronto como las circunstancias lo permitan. A fin de mantener alguna presión sobre las Partes y de que, como mínimo, consideren la posibilidad de retirar sus reservas, el párrafo 2 autoriza al Secretario General del Consejo de Europa a consultar

periódicamente a las Partes acerca de las probabilidades de retirarlas. Esa posibilidad de consulta es una práctica habitual en varios instrumentos del Consejo de Europa y se refleja en el artículo 43, párrafo 3, del Convenio y en el artículo 13, párrafo 2, del Primer Protocolo. De este modo, las Partes tienen la oportunidad de indicar si todavía necesitan mantener sus reservas con respecto a determinadas disposiciones y de retirar, más tarde, las que ya no sean necesarias. Se espera que, con el tiempo, las Partes puedan retirar el mayor número posible de reservas para promover la aplicación uniforme de este Protocolo.

Artículo 21 -Enmiendas

318. El artículo 21 sigue el mismo procedimiento previsto para las enmiendas en el artículo 44 del Convenio. Este procedimiento simplificado permite introducir enmiendas sin necesidad de negociar un Protocolo de enmienda en caso necesario. Queda entendido que los resultados de las consultas celebradas con las Partes en el Convenio en virtud del párrafo 3 del presente artículo no son vinculantes para las Partes en el Protocolo. Como se señala en el párrafo 323 del Informe explicativo del Convenio, "el procedimiento de enmienda está concebido principalmente para cambios relativamente menores de carácter procesal y técnico".

Artículo 22 - Solución de controversias

319. El artículo 22 dispone que los mecanismos de solución de controversias previstos en el artículo 45 del Convenio se aplicarán también al presente Protocolo (véase el párrafo 326 del Informe explicativo del Convenio).

Artículo 23 - Consultas de las Partes y evaluación de la aplicación

320. El párrafo 1 del artículo 23 dispone que el artículo 46 del Convenio (Consultas entre las Partes) es aplicable al presente Protocolo. Como se señala en el párrafo 327 del Informe explicativo del Convenio, el artículo 46 creó "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 modificar el Convenio". El procedimiento ha sido concebido en aras de la flexibilidad y se ha permitido a las Partes que decidan la manera y el momento de efectuar consultas. Tras la entrada en vigor del Convenio en 2004, las Partes comenzaron a realizar reuniones

periódicas en el marco del "Comité del Convenio sobre la Ciberdelincuencia" (T-CY). Con el tiempo, el T-CY, establecido de conformidad con el Artículo 46 y dotado de un Reglamento Interno adoptado por las Partes en el Convenio, realizó evaluaciones acerca de la aplicación del Convenio por las Partes, adoptó notas orientativas destinadas a facilitar una concepción común de las Partes en el presente Protocolo en cuanto a la utilización del Convenio, y preparó el proyecto del presente Protocolo. Los procedimientos para las consultas con las Partes siguen siendo flexibles y, por lo tanto, pueden ser adaptados por las Partes en el presente Protocolo, según proceda, para tener en cuenta las necesidades que puedan surgir en relación con la aplicación del presente Protocolo.

321. Al igual que en el Convenio (véase el párrafo 327 del Informe explicativo), las consultas en virtud del artículo 23 "examinarán en particular cuestiones que han surgido en cuanto a la utilización y la aplicación del Convenio, incluidos los efectos de las declaraciones y reservas formuladas". Esto podría incluir consultas y evaluación de la aplicación del presente Protocolo por parte de los Estados constituyentes o entidades territoriales similares de los Estados federales que hayan sido notificadas al Secretario General del Consejo de Europa en virtud del artículo 17, párrafo 2; en lo que respecta a las Partes que son miembros de la UE, podría incluir brindar información y realizar consultas con otras Partes en este Protocolo sobre la legislación aplicable de la UE respecto a la utilización y aplicación del presente Protocolo en relación con el artículo 15, párrafo 1.b. Además de las consultas a través del T-CY con arreglo a este artículo, que se abordan en el párrafo siguiente, las Partes pueden realizar consultas de forma bilateral. En el caso de los Estados federales, esas consultas y evaluaciones se realizarían a través de su gobierno central.

322. En el párrafo 2 del artículo 23 se establecen procedimientos específicos para evaluar la utilización y aplicación del Protocolo en el marco más amplio establecido por el artículo 46 y el T-CY como ya se ha mencionado. El párrafo 2 dispone que "las Partes evaluarán periódicamente la utilización y aplicación efectivas de las disposiciones del presente Protocolo" y señala que el artículo 2 del Reglamento Interno del Comité del Convenio sobre la Ciberdelincuencia, revisado el 16 de octubre de 2020, se aplicará *mutatis mutantis*. Esos procedimientos están disponibles en el sitio web del T-CY. Dado que el T-CY ha evaluado varias disposiciones del Convenio y ha presentado informes con arreglo a esos procedimientos, quienes participaron en la redacción estimaron que esos procedimientos bien establecidos se aplicarán *mutatis mutandis* a la evaluación de las disposiciones del presente Protocolo. En vista de las

obligaciones adicionales asumidas por las Partes en este Protocolo y de las medidas de cooperación particulares previstas en el mismo, quienes participaron en la redacción determinaron que esas evaluaciones corresponderían solo a las Partes en el presente Protocolo. Habida cuenta de los conocimientos técnicos necesarios para evaluar la utilización y la aplicación de algunas de las disposiciones del presente Protocolo, incluido el artículo 14 relativo a la protección de datos, las Partes podrán contemplar la posibilidad de que sus especialistas en la materia participen en las evaluaciones.

323. Mientras que, por un lado, las normas para esas evaluaciones deben ser previsibles, en la realidad la experiencia puede hacer necesaria la adaptación de esos procedimientos, sin que se requiera una enmienda oficial del presente Protocolo de conformidad con el artículo 21. Por lo tanto, el párrafo 2 establece que la revisión inicial de los procedimientos tendrá lugar cinco años después de la entrada en vigor del presente Protocolo, momento en el que las Partes podrán modificar esos procedimientos por consenso. Las Partes podrán modificar los procedimientos por consenso en cualquier momento después de esa revisión inicial.

324. Dada la relevancia de las salvaguardias de protección de los datos contenidas en el artículo 14, quienes participaron en la redacción consideraron que el artículo 14 debería ser evaluado tan pronto como hubiera un historial suficiente en cuanto a la cooperación en el marco de este Protocolo que permita examinar de manera eficaz la utilización y aplicación de esta disposición por las Partes. Por lo tanto, en el párrafo 3 se dispone que la revisión del artículo 14 se iniciará una vez que diez Partes en el Convenio hayan expresado su consentimiento en obligarse por el presente Protocolo.

Artículo 24 - Denuncia

325. Los párrafos 1 y 2 del artículo 24 son similares a los del párrafo 47 del Convenio y no requieren mayor explicación. El párrafo 3 establece que "la denuncia del Convenio por una Parte en el presente Protocolo constituye una denuncia del presente Protocolo". En vista del énfasis del presente Protocolo en el intercambio de información o de pruebas, que pueden incluir datos personales, quienes participaron en la redacción consideraron prudente añadir el párrafo 4 para aclarar que "la información o las pruebas transferidas antes de la fecha efectiva de la denuncia seguirán siendo tratadas de conformidad con el presente Protocolo.

Notas de orientación

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[15]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[16] El propósito es asegurar que las nuevas formas de delincuencia queden siempre cubiertas por el Convenio.

15. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
16. Párrafo 36 del Informe explicativo

Nota de orientación sobre la noción de "sistema informático"[17]

Artículo 1.a del Convenio de Budapest sobre la ciberdelincuencia

1. Introducción

En su primera reunión (Estrasburgo, 20 al 21 de marzo de 2006), el T-CY examinó el alcance de la definición de "sistema informático" en el artículo 1.a del Convenio de Budapest a la luz de las nuevas tecnologías que van más allá de los sistemas de ordenadores centrales y personales.

Desde la elaboración del Convenio, han surgido nuevos dispositivos tales como los teléfonos móviles de nueva generación o *smartphones*, los PDA, las tabletas y otros, que producen, procesan o transmiten datos. Es así como se ha hecho necesario definir si el concepto de "sistema informático" contemplado en el Convenio de Budapest abarca estos nuevos dispositivos.

En 2006, el T-CY convino en que los dispositivos en cuestión estaban cubiertos por la definición de "sistema informático" del apartado a) del artículo 1.

La presente nota de orientación afirma este entendimiento común de las partes, como se refleja en el informe de la primera reunión (documento T-CY(2006)11).

2. Artículo 1.a. del Convenio de Budapest sobre la ciberdelincuencia (CETS núm. 185)

Texto del Convenio

Artículo 1 – Definiciones

A los efectos del presente Convenio:

por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Extracto del Informe explicativo

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

17. Adoptado por el T-CY en su 8ª reunión plenaria (5 al 6 de diciembre de 2012).

(*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, tales como 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 ejemplo, alámbricas o por cable), inalámbricas (por ejemplo, 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.

3. Declaración del T-CY sobre la noción de "sistema informático" (apartado a) del artículo 1 del Convenio de Budapest)

Según la definición contenida en el apartado a) del artículo 1 del Convenio, por "sistema informático" se entenderá todo "dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa".

El T-CY conviene en que esta definición se extiende, por ejemplo, a los teléfonos móviles modernos, que tienen múltiples funciones, entre ellas, la capacidad de producir, procesar y transmitir datos, como ocurre al acceder a Internet, enviar correos electrónicos, transmitir archivos adjuntos, subir contenidos o descargar documentos.

Igualmente, reconoce que los ayudantes digitales personales, con o sin funcionalidad inalámbrica, también producen, procesan y transmiten datos.

El T-CY subraya que, cuando estos dispositivos realizan tales funciones, están procesando "datos informáticos" como se definen en el apartado b) del artículo 1. Además, estima que al ejecutar estas funciones, crean "datos sobre el tráfico", de acuerdo con la definición contenida en el apartado d) del artículo 1.

Por lo tanto, al procesar tales datos, actúan como un "sistema informático" según lo definido en el apartado a) del artículo 1.

El T-CY admite que esto concuerda con la interpretación de "sistema informático" que presenta el Informe explicativo, y que el Convenio cubrirá estos dispositivos de acuerdo con dicha capacidad.

4. Conclusión

El T-CY conviene en que la definición de "sistema informático" contenida en el apartado a) del artículo 1 abarca nuevas tecnologías que van más allá de los sistemas de ordenadores centrales y personales, como los teléfonos móviles modernos, *smartphones*, PDA, tabletas o semejantes.

Nota de orientación sobre disposiciones del Convenio de Budapest aplicables a las botnets[18]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[19]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

La presente nota aborda la cuestión de las botnets.

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[20] El propósito es asegurar que las nuevas formas de programas informáticos malintencionados o delincuencia queden siempre cubiertas por el Convenio.

Esta nota de orientación destaca cómo diferentes artículos del Convenio se aplican a las botnets.

2. Disposiciones pertinentes del Convenio de Budapest sobre la ciberdelincuencia (CETS núm. 185)

El término "botnet" se refiere a:

> "una red de ordenadores que han sido infectados por programas nocivos (virus informáticos). Esta red de ordenadores afectados (*zombies*) puede ser activada para realizar determinadas acciones como ataques a los sistemas de información (ciberataques). Los *zombies* pueden ser controlados —con frecuencia sin el conocimiento de los usuarios de los ordenadores afectados— por otro ordenador. El ordenador 'controlador' también se conoce como el 'centro de dirección y control'".[21]

---

18. Adoptada por la 9ª reunión plenaria del T-CY (4 al 5 junio de 2013).
19. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
20. Párrafo 36 del Informe explicativo
21. Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques a los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo [COM(2010) 517 final]

Una conexión entre ordenadores puede tener fines delictivos o lícitos.[22] En este sentido, no resulta relevante que las botnets sean redes de ordenadores. Lo que hay que destacar es que los ordenadores de las botnets se utilizan sin consentimiento, con fines delictivos y con el propósito de causar un impacto a gran escala.

Las botnets están cubiertas por las siguientes secciones del Convenio, en función de la acción efectiva de cada una. Cada disposición contempla un criterio relativo a la intención ("acto ilegítimo", "intención dolosa", etc.) que debe ser fácilmente demostrable cuando de se trata de botnets.

Artículos pertinentes	**Ejemplos**
Artículo 2 – Acceso ilícito	La creación y operación de una botnet supone el acceso ilícito a sistemas informáticos.[7] Las botnets pueden utilizarse para acceder de manera ilícita a otros sistemas informáticos.
Artículo 3 – Interceptación ilícita	Las botnets pueden utilizar medios técnicos para interceptar transmisiones no públicas de datos informáticos dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo.
Artículo 4 – Ataques a la integridad de los datos	La creación de una botnet siempre altera y puede dañar, borrar, deteriorar o suprimir datos informáticos. Las botnets como tales dañan, borran, deterioran, alteran o suprimen datos informáticos.
Artículo 5 – Ataques a la integridad del sistema	Las botnets pueden obstaculizar el funcionamiento de un sistema informático. Esto incluye los ataques de denegación de servicio distribuido.[8]

22. Las redes de ordenadores pueden crearse voluntariamente con fines delictivos. Los delitos cometidos mediante tales redes están cubiertos por el Convenio pero no son abordados en esta nota.
23. Véase también la Nota de orientación 1 sobre la noción de "sistema informático"
24. Véase la Nota de orientación respectiva.
25. Aun cuando formulen reservas con respecto al artículo 6, las partes tipificarán como delito la venta, distribución o puesta a disposición de los dispositivos contemplados en el mismo.

Artículos pertinentes	Ejemplos
Artículo 6 – Abuso de los dispositivos	Todas las botnets son dispositivos que responden a la definición del artículo 6 en la medida en que son concebidas o adaptadas principalmente para la comisión de los delitos previstos en los artículos 2 a 5.[9] El artículo 6 puede aplicarse también a los programas utilizados para la creación y el funcionamiento de botnets. Por lo tanto, el artículo 6 prevé la tipificación como delito de los actos de producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición, así como de posesión, de dispositivos como las botnets o los programas utilizados para su creación o funcionamiento.
Artículo 7 – Falsificación informática	Dependiendo del diseño de la botnet, esta puede introducir, alterar, borrar o suprimir datos informáticos y, de esta manera, generar datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como si fuesen auténticos.
Artículo 8 – Fraude informático	Las botnets pueden causar perjuicio patrimonial a una persona mientras que otra obtiene un beneficio económico mediante la introducción, alteración, borrado o supresión de datos informáticos o la interferencia en el funcionamiento de un sistema informático.
Artículo 9 – Delitos relacionados con la pornografía infantil	Las botnets pueden difundir materiales que implican la explotación de menores.
Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Las botnets pueden difundir ilegalmente datos protegidos por las leyes de propiedad intelectual.

Artículos pertinentes	Ejemplos
Artículo 11 – Tentativa y complicidad	Las botnets pueden ser utilizadas para tratar de cometer varios de los delitos previstos en el Convenio o para hacerse cómplice de estos.
Artículo 13 – Sanciones y medidas	Las botnets son utilizadas con distintos fines delictivos, algunos de los cuales tienen un fuerte impacto sobre los individuos, las instituciones del sector público o el sector privado, o sobre infraestructuras críticas. No obstante, puede suceder que alguna de las Partes prevea en su derecho interno una sanción insuficientemente severa para los delitos relacionados con las botnets y que no permita tomar en consideración las circunstancias agravantes, la tentativa o la complicidad. En tal caso, podría ser necesario que se modifique la legislación nacional. Así, con arreglo a lo dispuesto por el artículo 13, las Partes deberían garantizar que los delitos relacionados con las botnets estén sujetos a "sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Para las personas jurídicas, esto puede significar sanciones penales o no penales, incluidas sanciones pecuniarias.
	Las Partes también pueden tener en cuenta circunstancias agravantes, por ejemplo si las botnets afectan a un gran número de sistemas o si los ataques causan perjuicios considerables, como muertes, lesiones físicas o daño a infraestructuras críticas.

3. Declaración del T-CY

La lista anterior de artículos en relación con las botnets ilustra la diversidad de delitos que se pueden cometer mediante estas redes y las disposiciones penales que pueden aplicarse.

Por lo tanto, el T-CY conviene en que los diferentes aspectos relativos a las botnets están cubiertos por el Convenio de Budapest.

Nota de orientación sobre los ataques de denegación de servicio distribuido (DDOS)[26]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[27]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

La presente nota aborda la cuestión de los ataques de denegación de servicio (DOS) y denegación de servicio distribuido (DDOS).

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[28] El propósito es asegurar que las nuevas formas de programas informáticos malintencionados o delincuencia queden siempre cubiertas por el Convenio.

Esta nota de orientación destaca cómo diferentes artículos del Convenio se aplican a los ataques DOS y DDOS.

2. Disposiciones pertinentes del Convenio de Budapest sobre la ciberdelincuencia (CETS núm. 185)

Los ataques de denegación de servicio (DOS) utilizan diferentes medios para impedir que un sistema informático esté disponible para los usuarios. Uno de estos medios puede ser la saturación de los ordenadores o las redes que son blanco del ataque, a través de solicitudes de comunicación externas que obstaculizan el servicio a usuarios legítimos. Los ataques de denegación de servicio distribuido (DDOS) son ataques de denegación de servicio ejecutados por muchos ordenadores al mismo tiempo. Actualmente, existen diferentes formas comunes de lanzar ataques DOS o DDOS, por ejemplo: enviar solicitudes distorsionadas a un sistema informático, superar el límite de capacidad

26. Adoptada por la 9ª reunión plenaria del T-CY (4 al 5 junio de 2013).
27. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
28. Párrafo 36 del Informe explicativo

de usuarios, o enviar a servidores de correo electrónico más mensajes de los que pueden recibir y tratar.

Los ataques DOS y DDOS están cubiertos por las siguientes secciones del Convenio, en función de la acción efectiva de cada uno. Cada disposición contempla un criterio relativo a la intención ("acto ilegítimo", "intención dolosa", etc.) que debe ser fácilmente demostrable en los casos de DOS y DDOS.

3. Interpretación del T-CY relativa a la penalización de los ataques DDOS

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	Mediante los ataques DOS y DDOS, se puede tener acceso a un sistema informático.
Artículo 4 – Ataques a la integridad de los datos	Los ataques DOS y DDOS pueden dañar, borrar, deteriorar, alterar o suprimir datos informáticos.
Artículo 5 – Ataques a la integridad del sistema	El objetivo de un ataque DOS o DDOS es justamente la obstaculización grave del funcionamiento de un sistema informático.
Artículo 11 – Tentativa y complicidad	Los ataques DOS y DDOS pueden ser utilizados para tratar de cometer varios de los delitos previstos en el Convenio o para hacerse cómplice de estos (por ejemplo, falsificación informática, artículo 7; fraude informático, artículo 8; delitos relacionados con la pornografía infantil, artículo 9, y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, artículo 10).
Artículo 13 – Sanciones y medidas	Los ataques DOS y DDOS pueden representar un peligro en muchos sentidos, en particular cuando su blanco son sistemas cruciales para la vida diaria (por ejemplo, si afectan a sistemas bancarios u hospitalarios). Puede suceder que alguna de las Partes prevea en su derecho interno una sanción insuficientemente severa para los ataques DOS o DDOS, y que no permita tomar en consideración las circunstancias agravantes, la tentativa o la complicidad.

Artículos pertinentes	Ejemplos
	En tal caso, podría ser necesario que se modifique la legislación nacional. Con arreglo a lo dispuesto en el artículo 13, las Partes deberían garantizar que los delitos relacionados con los ataques en cuestión "estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Para las personas jurídicas, esto puede significar sanciones penales o no penales, incluidas sanciones pecuniarias. Las Partes también pueden tener en cuenta circunstancias agravantes, por ejemplo si los ataques DOS o DDOS afectan a una gran cantidad de sistemas o causan perjuicios considerables, como muertes, lesiones físicas o daño a infraestructuras críticas.

4. Declaración del T-CY

La lista anterior de artículos en relación con los ataques DOS y DDOS ilustra la diversidad de delitos que se pueden cometer mediante estos ataques.

Por lo tanto, el T-CY conviene en que los diferentes aspectos de los ataques en cuestión están cubiertos por el Convenio de Budapest.

Nota de orientación sobre usurpación de identidad y suplantación de identidad en relación con fraude[29]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[30]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

La presente nota hace referencia a la usurpación de identidad, la suplantación de identidad (*phishing*) y los actos[31] afines en relación con fraude.

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[32] El propósito es asegurar que las nuevas formas de delincuencia queden siempre cubiertas por el Convenio.

Esta nota de orientación destaca cómo diferentes artículos del Convenio se aplican a la usurpación de identidad en relación con fraude mediante sistemas informáticos.

2. Usurpación de identidad y suplantación de identidad

Si bien no existe una definición generalmente aceptada ni un uso constante del término "usurpación de identidad", éste suele hacer referencia a actos delictivos que consisten en obtener y utilizar la información de identidad de una persona de modo fraudulento (sin su conocimiento o consentimiento). El término "fraude de identidad" se emplea algunas veces como sinónimo, aunque este abarca también el uso de una identidad falsa, que no es necesariamente real.

---

29. Adoptada por la 9ª reunión plenaria del T-CY (4 al 5 junio de 2013).
30. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
31. Los actos afines al *phishing* se conocen con diferentes nombres como: *spear phishing*, *SMiShing*, *pharming* y *vishing*.
32. Párrafo 36 del Informe explicativo

La información de identidad de una persona real o ficticia puede usarse para cometer actos ilícitos de diversa índole. Sin embargo, la presente nota de orientación se centra en la usurpación de identidad en relación con fraude únicamente.

Esto puede implicar la apropiación indebida de la identidad de otra persona (por ejemplo, nombre, fecha de nacimiento, dirección actual o direcciones anteriores), sin su conocimiento o consentimiento. La información de identidad se utiliza entonces para obtener bienes y servicios en nombre de esa persona.

Algunos actos relacionados pueden ser el *phishing*, el *pharming*, el *spear phishing*, el *spoofing* o conductas similares, por ejemplo con fines de obtener contraseñas u otros datos de acceso, a menudo mediante correo electrónico o sitios web falsos.

La usurpación de identidad afecta a gobiernos, empresas y ciudadanos, y provoca importantes daños, además de minar la confianza en las tecnologías de la información.

En muchos sistemas jurídicos, no existe un delito específico de usurpación de identidad. Quienes cometen actos de usurpación de identidad suelen ser acusados de delitos más graves (por ejemplo, fraude financiero). La obtención de una identidad falsa implica por lo general la comisión de un delito como la falsificación de documentos o la alteración de datos informáticos. Una identidad falsa facilita muchos delitos, como la inmigración ilegal, la trata de seres humanos, el blanqueo de dinero, el tráfico de estupefacientes y el fraude financiero contra gobiernos o contra el sector privado. No obstante, lo más común es que se utilice en relación con el fraude.

Desde el punto de vista conceptual, la usurpación de identidad se puede dividir en tres fases:

- Fase 1 – La obtención de información de identidad, por ejemplo mediante robo físico, motores de búsqueda, ataques desde el interior o desde el exterior (acceso ilícito a sistemas informáticos, troyanos, registradores de teclado, software espía y otros programas informáticos malintencionados), o mediante suplantación de identidad u otras técnicas de ingeniería social.
- Fase 2 – La posesión y cesión de información de identidad, lo cual incluye la venta de dicha información a terceros.
- Fase 3 – El uso de información de identidad para cometer fraude u otros delitos, por ejemplo utilizando la identidad de otra persona para explotar

cuentas bancarias y tarjetas de crédito, crear nuevas cuentas, solicitar préstamos o créditos, adquirir bienes y servicios o difundir programas informáticos malintencionados.

Como conclusión, la usurpación de identidad (incluidas la suplantación de identidad y las conductas similares) sirve generalmente para preparar otros actos delictivos como el fraude informático. Aunque la usurpación de identidad no esté tipificada como delito independiente, las autoridades competentes podrán procesar a los autores por los delitos subsiguientes.

3. Interpretación del T-CY relativa a la penalización de la usurpación de identidad en relación con fraude en el marco del Convenio de Budapest

El Convenio de Budapest se centra en las conductas delictivas y no en las técnicas o tecnologías empleadas propiamente dichas. Por lo tanto, no contiene disposiciones específicas sobre la usurpación de identidad o la suplantación de identidad. No obstante, la plena aplicación de las disposiciones de derecho sustantivo permitirá a los Estados penalizar las conductas relacionadas con la usurpación de identidad.

El Convenio exige a los Estados penalizar conductas como el acceso ilícito a un sistema informático, la interceptación ilícita de datos, los ataques a la integridad de los datos, los ataques a la integridad del sistema, el abuso de los dispositivos y el fraude informático:

Fases	Artículos del convenio	Ejemplos
Fase 1 – Obtención de la información de identidad	Artículo 2 – Acceso ilícito	En los actos de usurpación de identidad o suplantación de identidad, puede haber acceso ilícito a un sistema informático cuando el autor "piratea", evita una protección por contraseña, registra las pulsaciones de un teclado o aprovecha los defectos de un software. El acceso ilícito a sistemas informáticos es uno de los delitos más comunes cuando se trata de obtener información sensible como la de identidad.

Fases	Artículos del convenio	Ejemplos
	Artículo 3 – Interceptación ilícita	La usurpación de identidad implica a menudo el uso de registradores de teclado (*keyloggers*) u otros tipos de programas informáticos malintencionados para la interceptación ilícita de transmisiones no públicas de datos informáticos dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo que contienen información sensible como la relacionada con la identidad.
	Artículo 4 – Ataques a la integridad de los datos	La usurpación de identidad o la suplantación de identidad pueden dañar, borrar, deteriorar, alterar o suprimir datos informáticos. La usurpación de identidad o la suplantación de identidad pueden implicar que se obstaculice el funcionamiento de un sistema informático con el objetivo de robar o facilitar el robo de información de identidad.
	Artículo 5 – Ataques a la integridad del sistema	Con frecuencia, esto ocurre durante el proceso de acceso ilícito cuando se instala un registrador de teclado para obtener información sensible.
	Artículo 7 – Falsificación informática	La usurpación de identidad o la suplantación de identidad pueden implicar la introducción, alteración, borrado o supresión de datos informáticos y, de esta manera, tener como resultado que datos que no son auténticos sean tomados o utilizados como si lo fuesen. La suplantación de identidad es quizás la forma más común de falsificación informática (por ejemplo, falsificación del sitio web de una institución financiera) y, por ende, la actividad ilícita a través de la cual se recoge más información sensible como la de identidad.

Fases	Artículos del convenio	Ejemplos
Fase 2 – Posesión y cesión de información de identidad	Artículo 6 – Abuso de los dispositivos	El robo de información de identidad (por ejemplo, contraseñas, datos de acceso, tarjetas de crédito) se puede considerar a la luz de este artículo como el abuso de un "dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los anteriores artículos 2 a 5", o de "una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático".
Fase 3 – Uso de la información de identidad para cometer fraude u otros delitos	Artículo 8 – Fraude informático	El uso de una identidad falsa mediante la introducción, alteración, borrado o supresión de datos informáticos o la interferencia en el funcionamiento de un sistema informático permite explotar cuentas bancarias o tarjetas de crédito, solicitar préstamos o créditos, o adquirir bienes y servicios. De este modo, dicho uso puede causar un perjuicio patrimonial a una persona mientras que otra obtiene un beneficio económico.
Todas las fases	Artículo 11 – Tentativa y complicidad	La obtención, posesión y cesión de información de identidad puede constituir tentativa o complicidad con vistas a cometer varios de los delitos previstos por el Convenio.
	Artículo 13 – Sanciones y medidas	La usurpación de identidad es utilizada con distintos fines delictivos, algunos de los cuales perjudican gravemente a los individuos y a instituciones del sector público o el sector privado. No obstante, puede suceder que alguna de las Partes prevea en su derecho interno una sanción insuficientemente severa para la usurpación de identidad y que no permita tomar en consideración las circunstancias agravantes.

Fases	Artículos del convenio	Ejemplos
		En tal caso, podría ser necesario que se modifique la legislación nacional. Así, con arreglo a lo dispuesto por el artículo 13, las Partes deberían garantizar que los delitos relacionados con la usurpación de identidad "estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Para las personas jurídicas, esto puede significar sanciones penales o no penales, incluidas sanciones pecuniarias. Asimismo, las Partes pueden tener en cuenta circunstancias agravantes, por ejemplo si la usurpación de identidad afecta a una gran cantidad de personas, causa dificultades graves o pone en peligro a una persona.

4. Declaración del T-CY

El T-CY admite que lo anterior refleja los distintos elementos y el alcance de la usurpación de identidad y la suplantación de identidad, así como las disposiciones penales que podrían aplicarse.

Por lo tanto, el T-CY conviene en que los diferentes aspectos de estos actos están cubiertos por el Convenio de Budapest.

Nota de orientación sobre los ataques a infraestructuras críticas de información[33]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[34]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

La presente nota aborda la cuestión de los ataques a infraestructuras críticas de información.

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[35] El propósito es asegurar que las nuevas formas de programas informáticos malintencionados o delincuencia queden siempre cubiertas por el Convenio.

Esta nota de orientación destaca cómo diferentes artículos del Convenio se aplican a los ataques a infraestructuras críticas de información.

2. Disposiciones pertinentes del Convenio de Budapest sobre la ciberdelincuencia (CETS núm. 185)

Las infraestructuras críticas pueden definirse como sistemas y bienes, sean estos físicos o virtuales, que resultan vitales para un país, a tal punto que su interrupción, mal funcionamiento o destrucción puede tener un efecto perjudicial desde el punto de vista de la defensa y la seguridad nacional, la seguridad económica, la salud y el orden público, o cualquier combinación de estos aspectos. Si bien cada país determina sus propias infraestructuras críticas, muchos consideran que estas abarcan los sectores relacionados con la energía, la alimentación, el agua, el combustible, el transporte, las comunicaciones, las finanzas, la industria, la defensa y los servicios públicos y gubernamentales.

33. Adoptada por la 9ª reunión plenaria del T-CY (4 al 5 junio de 2013).
34. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
35. Párrafo 36 del Informe explicativo

Con frecuencia, las infraestructuras críticas son gestionadas mediante sistemas informáticos, incluidos los llamados sistemas de control industrial (SCI) o sistemas de supervisión, control y adquisición de datos (SCADA). En general, dichos sistemas se conocen como infraestructuras críticas de información.

Fuentes privadas y gubernamentales afirman que cada año en el mundo se produce una cantidad importante, aunque desconocida, de ataques a infraestructuras críticas de información. Aunque estos ataques se valen de las mismas técnicas que otros delitos electrónicos, la manera en que afectan a la sociedad es distinta: pueden agotar fondos del Tesoro público, paralizar sistemas de agua, perturbar el control del tráfico aéreo, etc.

Las formas actuales y futuras de ataques a infraestructuras críticas de información están cubiertas por las siguientes secciones del Convenio, dependiendo de la naturaleza del ataque. Cada disposición contempla un criterio relativo a la intención ("acto ilegítimo", "intención dolosa", etc.) que se debe tener en cuenta a la hora de determinar las modalidades de penalización.

3. Interpretación del T-CY relativa a la penalización de los ataques a infraestructuras críticas de información

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	Los ataques a infraestructuras críticas de información pueden significar el acceso a un sistema informático.
Artículo 3 – Interceptación ilícita	Los ataques a infraestructuras críticas de información pueden utilizar medios técnicos para interceptar transmisiones no públicas de datos informáticos dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo.
Artículo 4 – Ataques a la integridad de los datos	Los ataques a infraestructuras críticas de información pueden dañar, borrar, deteriorar, alterar o suprimir datos informáticos.
Artículo 5 – Ataques a la integridad del sistema	Los ataques a infraestructuras críticas de información pueden obstaculizar el funcionamiento de un sistema informático. De hecho, este puede ser su objetivo principal.

Artículos pertinentes	Ejemplos
Artículo 7 – Falsificación informática	Los ataques a infraestructuras críticas de información pueden introducir, alterar, borrar o suprimir datos informáticos y, de esta manera, generar datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como si fuesen auténticos.
Artículo 8 – Fraude informático	Los ataques a infraestructuras críticas de información pueden causar perjuicio patrimonial a una persona mientras que otra obtiene un beneficio económico mediante la introducción, alteración, borrado o supresión de datos informáticos o la interferencia en el funcionamiento de un sistema informático.
Artículo 11 – Tentativa y complicidad	Los ataques a infraestructuras críticas de información pueden ser utilizados para tratar de cometer varios de los delitos previstos en el Convenio o para hacerse cómplice de estos.
Artículo 13 – Sanciones y medidas	Los efectos de los ataques a infraestructuras críticas de información son diversos (pueden variar en cada país por razones técnicas, culturales o de otra índole), pero normalmente los gobiernos se ocupan de estos cuando causan daños graves o generalizados. Puede suceder que una Parte prevea en su derecho interno una sanción insuficientemente severa para los ataques a infraestructuras críticas de información, y que no permita tomar en consideración las circunstancias agravantes, la tentativa o la complicidad. En tal caso, podría ser necesario que se modifique la legislación nacional. Con arreglo a lo dispuesto en el artículo 13, las Partes deberían garantizar que los delitos relacionados con los ataques en cuestión "estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Para las personas jurídicas, esto puede significar sanciones penales o no penales, incluidas sanciones pecuniarias.

Artículos pertinentes	Ejemplos
	Las Partes también pueden tener en cuenta circunstancias agravantes, por ejemplo si los ataques a infraestructuras críticas de información afectan a una gran cantidad de sistemas o causan perjuicios considerables, como muertes o lesiones físicas.

4. Declaración del T-CY

La lista anterior de artículos en relación con los ataques a infraestructuras críticas de información ilustra la diversidad de delitos que se pueden cometer mediante dichos ataques.

Por lo tanto, el T-CY conviene en que los diferentes aspectos de los ataques en cuestión están cubiertos por el Convenio de Budapest.

Nota de orientación sobre nuevas formas de programas informáticos malintencionados[36]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[37]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

La presente nota aborda la cuestión de las nuevas formas de programas informáticos malintencionados (*malware*).

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[38] El propósito es asegurar que las nuevas formas de programas informáticos malintencionados o delincuencia queden siempre cubiertas por el Convenio.

Esta nota de orientación destaca cómo diferentes artículos del Convenio se aplican a las nuevas formas de programas informáticos malintencionados.

2. Disposiciones pertinentes del Convenio de Budapest sobre la ciberdelincuencia (CETS núm. 185)

Actualmente, existen muchas formas de programas informáticos malintencionados, *malware*. Según la Organización para la Cooperación y el Desarrollo Económicos, este es "un término general para definir una pieza de software insertada en un sistema de información para dañar ése u otros sistemas o utilizarlos con otros fines".[39] Las formas más conocidas son los gusanos, virus y troyanos. Los programas informáticos malintencionados de hoy, pueden robar datos copiándolos y enviándolos a otra dirección; pueden manipular datos; pueden obstaculizar el funcionamiento de sistemas informáticos, incluidos los que controlan infraestructuras críticas; pueden borrar, suprimir o bloquear el

36. Adoptada por la 9ª reunión plenaria del T-CY (4 al 5 junio de 2013).
37. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
38. Párrafo 36 del Informe explicativo
39. Véase: http://www.oecd.org/internet/ieconomy/40724457.pdf

acceso a datos, como es el caso de los programas de extorsión (*ransomware*), y, mediante un diseño especial, pueden afectar a sistemas informáticos específicos.

Según fuentes privadas y gubernamentales, cada año se desarrollan y descubren ingentes cantidades de nuevas formas de programas informáticos malintencionados, cuyos objetivos son diversos. Estas nuevas formas, al igual que las antiguas, pueden servir para robar dinero, interrumpir sistemas de agua, amenazar a usuarios, etc.

Las formas de *malware* son tan numerosas y diversas que no sería posible describir en una normativa penal ni siquiera aquellas que se conocen hoy en día. El Convenio sobre la ciberdelincuencia evita deliberadamente términos como gusano, virus o troyano. Teniendo en cuenta que los programas informáticos malintencionados evolucionan continuamente, la utilización de tales términos en el Convenio lo haría rápidamente obsoleto y sería contraproducente.

Por supuesto, tampoco es posible describir en una normativa todas las formas futuras.

Por eso, en lo que atañe a los programas informáticos malintencionados, es importante centrarse en los objetivos que persiguen y en sus efectos, los cuales ya son conocidos y sí pueden ser descritos en una normativa.

Las formas actuales y futuras de *malware* están contempladas en las siguientes secciones del Convenio, en función de la acción efectiva de tales programas. Cada disposición contempla un criterio relativo a la intención ("acto ilegítimo", "intención dolosa", etc.) que se debe tener en cuenta a la hora de determinar las modalidades de penalización.

3. Interpretación del T-CY relativa a la penalización de las nuevas formas de programas informáticos malintencionados

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	Los programas informáticos malintencionados se pueden utilizar para tener acceso a sistemas informáticos.
Artículo 3 – Interceptación ilícita	Los programas informáticos malintencionados pueden utilizar medios técnicos para interceptar transmisiones no públicas de datos informáticos dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo.

Artículos pertinentes	Ejemplos
Artículo 4 – Ataques a la integridad de los datos	Los programas informáticos malintencionados dañan, borran, deterioran, alteran o suprimen datos informáticos.
Artículo 5 – Ataques a la integridad del sistema	Los programas informáticos malintencionados pueden obstaculizar el funcionamiento de un sistema informático.
Artículo 6 – Abuso de los dispositivos	Los programas informáticos malintencionados son dispositivos en el sentido del artículo 6 (aun cuando formulen reservas con respecto al artículo 6, las partes tipificarán como delito la venta, distribución o puesta a disposición de los dispositivos contemplados en el mismo). La razón es que son concebidos o adaptados principalmente para cometer los delitos previstos en los artículos 2 a 5. Además, el artículo 6 prevé la tipificación como delito de los actos de venta, obtención
	para su utilización, importación, difusión u otra forma de puesta a disposición de contraseñas, códigos de acceso o datos similares que puedan dar acceso a sistemas informáticos. Estos elementos suelen estar presentes en los casos de procesamiento relacionados con programas informáticos malintencionados.
Artículo 7 – Falsificación informática	Los programas informáticos malintencionados pueden introducir, alterar, borrar o suprimir datos informáticos y, de esta manera, generar datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como si fuesen auténticos.
Artículo 8 – Fraude informático	Los programas informáticos malintencionados pueden causar perjuicio patrimonial a una persona mientras que otra obtiene un beneficio económico mediante la introducción, alteración, borrado o supresión de datos informáticos o la interferencia en el funcionamiento de un sistema informático.

Artículos pertinentes	Ejemplos
Artículo 11 – Tentativa y complicidad	Los programas informáticos malintencionados pueden ser utilizados para tratar de cometer varios de los delitos previstos en el convenio o para hacerse cómplice de estos.
Artículo 13 – Sanciones y medidas	Los efectos de las nuevas formas de programas informáticos malintencionados son muy diversos. Algunos de estos programas son relativamente inofensivos, mientras que otros constituyen un peligro para las personas o las infraestructuras críticas, entre otros. Los efectos pueden variar en cada país por razones técnicas, culturales o de otra índole. Puede suceder que una Parte prevea en su derecho interno una sanción insuficientemente severa para los programas informáticos malintencionados, y que no permita tomar en consideración las circunstancias agravantes, la tentativa o la complicidad. En tal caso, podría ser necesario que se modifique la legislación nacional. Con arreglo a lo dispuesto en el artículo 13, las Partes deberían garantizar que los delitos relacionados con los ataques en cuestión "estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Para las personas jurídicas, esto puede significar sanciones penales o no penales, incluidas sanciones pecuniarias. Las Partes también pueden tener en cuenta circunstancias agravantes, por ejemplo si los programas informáticos malintencionados afectan a una gran cantidad de sistemas o causan perjuicios considerables, como muertes, lesiones físicas o daño a infraestructuras críticas.

4. Declaración del T-CY

La lista anterior de artículos en relación con todas las formas de programas informáticos malintencionados ilustra la diversidad de delitos que se pueden cometer mediante dichos programas.

Por lo tanto, el T-CY conviene en que los diferentes aspectos de todas las formas de programas informáticos malintencionados están cubiertos por el Convenio de Budapest.

Nota de orientación sobre el acceso transfronterizo a los datos (Artículo 32)[40]

1. Introducción

En su 8ª sesión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió publicar unas Notas de orientación encaminadas a facilitar la utilización y la aplicación efectivas del Convenio sobre la ciberdelincuencia (Convenio de Budapest), también a la luz de las novedades jurídicas, políticas y tecnológicas.[41]

Las Notas de orientación representan el entendimiento común de las Partes en este tratado en lo que respecta a la utilización del Convenio.

En la presente Nota se aborda la cuestión del acceso transfronterizo a los datos en virtud del artículo 32 del Convenio de Budapest.[42]

El apartado b) del artículo 32 es una excepción al principio de territorialidad, y permite el acceso transfronterizo unilateral sin necesidad de asistencia mutua en circunstancias limitadas. Se alienta a las Partes a utilizar de una manera más eficaz todas las disposiciones del Convenio de Budapest relativas a la cooperación internacional, incluida la asistencia mutua.

En general, las prácticas, los procedimientos y las condiciones y salvaguardias varían considerablemente entre los diferentes Estados. Persisten, y deben abordarse, las preocupaciones relativas a los derechos procesales de los sospechosos, a la privacidad y a la protección de los datos personales, a la base jurídica para acceder a los datos almacenados en jurisdicciones extranjeras o "en la nube", y a la soberanía nacional.

El objetivo de esta Nota de orientación es facilitar la aplicación del Convenio de Budapest por los Estados, corregir errores de comprensión en lo tocante al acceso transfronterizo en el marco de este tratado, y tranquilizar a terceros.

---

40. Adoptado por la 12ª sesión plenaria del T-CY.
41. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
42. La preparación de esta Nota de orientación representa el seguimiento de las conclusiones del informe sobre "Transborder access and jurisdiction" (T-CY(2012)3), adoptado por la sesión plenaria del T-CY en diciembre de 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

Así pues, la Nota de orientación ayudará a los Estados a aprovechar plenamente el potencial del tratado con respecto al acceso transfronterizo a los datos.

2. Artículo 32 del Convenio de Budapest

Texto de la disposición:

> Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público
>
> Una Parte podrá, sin autorización de otra Parte:
>
> a tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos, o
>
> b tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Extracto del Informe explicativo

> 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 párrafo 3 del artículo 39 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.

3. Interpretación del T-CY del artículo 32 del Convenio de Budapest

En lo que respecta al apartado a) del artículo 32 (acceso transfronterizo a datos informáticos almacenados accesibles al público), no se han planteado cuestiones específicas ni se requiere más orientación del T-CY en estos momentos.

Normalmente se reconoce que las autoridades encargadas de hacer cumplir la ley pueden acceder a cualquier dato que sea accesible al público, y suscribirse o registrarse a tales efectos en servicios accesibles al público.[43]

Si una parte de un sitio web público, de un servicio o de algo similar se cierra al público, entonces no se considera accesible al público en el sentido del apartado a) del artículo 32.

Por lo referente al apartado b) del artículo 32, las situaciones típicas comprenden las siguientes:

- 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.[44]
- Un presunto traficante de drogas es arrestado legítimamente cuando su buzón de correo – que posiblemente contiene pruebas de un delito – está abierto en su tableta, su *smartphone* u otro dispositivo. Si el sospechoso expresa voluntariamente su consentimiento para que la policía acceda a la cuenta, y si la policía está segura de que los datos del buzón de correo

43. Sin embargo, la legislación nacional puede limitar el acceso de las autoridades encargadas de hacer cumplir la ley a los datos accesibles al público, o su utilización de los mismos.
44. Párrafo 294 del Informe explicativo.

están almacenados en otro Estado, la policía podrá acceder a los datos conformemente a lo previsto en el apartado b) del artículo 32.

No se autorizan ni se excluyen otras situaciones.[45]

En lo que respecta al apartado b) del artículo 32 (acceso transfronterizo con consentimiento), el T-CY comparte el siguiente entendimiento común:

Consideraciones generales y salvaguardias

El apartado b) del artículo 32 es una medida que debe aplicarse en investigaciones y procedimientos penales específicos en el ámbito de aplicación del artículo 14.[46]

Como se ha señalado anteriormente, se supone que las Partes en el Convenio constituyen una comunidad de confianza, y que el Estado de derecho y los principios de derechos humanos se respetan con arreglo a lo dispuesto en el artículo 15 del Convenio de Budapest.[47]

---

45. Párrafo 293 del Informe explicativo. Véase asimismo el párrafo 3 del artículo 39 del Convenio de Budapest.
46. Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento
    1 Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias con miras a establecer los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.
    2 Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:
    a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
    b. a cualquier otro delito cometido por medio de un sistema informático, y
    c. a la obtención de pruebas electrónicas de cualquier delito.
    3 a. Cualquier Parte podrá reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.
    b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:
        i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y
        ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.
47. Artículo 15 – Condiciones y salvaguardias
    1 Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y salvaguardias

Al aplicar la medida, deben tenerse en cuenta los derechos de las personas y los intereses de terceros.

Por lo tanto, un Estado que realiza una búsqueda puede contemplar la posibilidad de notificar a las autoridades competentes del Estado objeto de la búsqueda.

Acerca de la noción de "transfronterizo" y de "ubicación"

Acceso transfronterizo significa "acceder de forma unilateral a los datos informáticos almacenados en otra Parte sin solicitar la asistencia mutua".[48]

La medida pueda aplicarse entre las Partes.

El apartado b) del artículo 32 hace referencia a "datos informáticos almacenados en otro Estado". Esto implica que se puede utilizar el apartado b) del artículo 32 si se sabe dónde están ubicados los datos.

El apartado b) del artículo 32 no contemplaría las situaciones en las que los datos no están almacenados en otro Estado, o en los que no se sepa a ciencia cierta su ubicación. Un Estado no puede ampararse en el apartado b) del artículo 32 para conseguir que se revelen los datos que están almacenados a nivel nacional.

En virtud del apartado b) del artículo 32, no se autorizan ni excluyen otras situaciones. Por consiguiente, en los casos en los que se desconoce, o no se sabe a ciencia cierta, si los datos están almacenados en otro Estado, las Partes tal vez deban evaluar ellas mismas la legitimidad de una búsqueda o de otro tipo de acceso a la luz de la legislación nacional, los principios pertinentes del derecho internacional o las consideraciones de las relaciones internacionales.

---

previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2 Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3 Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

48. Párrafo 293 del Informe explicativo del Convenio de Budapest.

Acerca de la noción de "acceso sin autorización de otra Parte"

El apartado b) del artículo 32 no exige la asistencia mutua, y el Convenio de Budapest no exige una notificación de la otra Parte. Al mismo tiempo, el Convenio de Budapest no excluye la notificación. Las Partes pueden notificar a la otra Parte si lo consideran oportuno.

Acerca de la noción de "consentimiento"

El apartado b) del artículo 32 prevé que el consentimiento debe ser lícito y voluntario, lo que significa que no se puede obligar ni engañar a la persona que proporciona el acceso a los datos o que está de acuerdo con revelarlos.[49]

A reserva de la legislación nacional, un menor no podrá expresar su consentimiento, ni tampoco las personas que padecen enfermedades mentales o de otro tipo.

En la mayoría de los Estados, la cooperación en la investigación penal requeriría el consentimiento explícito. Por ejemplo, el acuerdo general de una persona con las condiciones de un servicio en línea utilizado tal vez no constituya consentimiento explícito, aun cuando estas condiciones indiquen que los datos pueden compartirse con las autoridades de justicia penal en caso de abuso.

Acerca de la legislación aplicable

En todos los casos, las autoridades encargadas de hacer cumplir la ley deben aplicar las mismas normas jurídicas establecidas de conformidad con el apartado b) del artículo 32 que aplicarían a nivel nacional. Si el acceso a los datos o su revelación no se permitiera a escala nacional, tampoco se permitiría en virtud del apartado b) del artículo 32.

Se supone que las Partes en el Convenio constituyen una comunidad de confianza, y que el Estado de derecho y los principios de derechos humanos se respetan de conformidad con el artículo 15 del Convenio de Budapest.

Acerca de la persona que puede proporcionar acceso a los datos o revelarlos

En lo que respecta a "quién" es la persona "autorizada legítimamente" a revelar los datos, esto puede variar en función de las circunstancias y de la legislación aplicable.

---

49. En algunos países, permitir que se eviten o reduzcan los cargos penales o una pena de prisión también constituye consentimiento lícito y voluntario.

Por ejemplo, puede tratarse de un particular, que proporcione acceso a su cuenta de correo electrónico o a otros datos que ha almacenado en el extranjero.[50]

También puede ser una persona jurídica.

Es improbable que los proveedores de servicios puedan expresar su consentimiento de manera válida y voluntaria para que se revelen los datos de sus usuarios de conformidad con el artículo 32. Por lo general, se limitarán a conservar los datos; no controlarán ni serán dueños de los datos y, por lo tanto, no estarán en condiciones de expresar su consentimiento de una manera válida. Por supuesto, los organismos encargados de hacer cumplir la ley tal vez puedan obtener datos a nivel transnacional recurriendo a otros métodos, como la asistencia jurídica mutua o procedimientos para situaciones de emergencia.

Solicitudes legítimas nacionales contra el apartado b) del artículo 32

El apartado b) del artículo 32 no es pertinente para las órdenes de presentación nacionales o para solicitudes legitimas similares que puede formular un Estado.

Acerca de la ubicación de la persona que expresa su consentimiento para que se acceda a los datos o para que éstos se revelen

La hipótesis estándar es que la persona que proporciona acceso está físicamente ubicada en el territorio de la Parte requirente.

Sin embargo, existen múltiples situaciones posibles. Podría ser que la persona física o jurídica esté ubicada en el territorio de la autoridad requirente encargada de hacer cumplir la ley al expresar su acuerdo para que se revelen los datos o al proporcionar efectivamente acceso a los mismos, o sólo al expresar su acuerdo para que se revelen los datos, pero no al proporcionar acceso a estos últimos, o que la persona esté ubicada en el país en el que se almacenan los datos al expresar su acuerdo para que se revelen los datos y al proporcionar acceso a estos últimos. La persona también puede estar físicamente ubicada en un tercer país al expresar su acuerdo para cooperar o al proporcionar efectivamente acceso a los datos. Si se trata de una persona jurídica (como una entidad del sector privado), esta persona puede estar

50. Véase el ejemplo proporcionado en el párrafo 294 del Informe explicativo.

representada en el territorio de la autoridad requirente encargada de hacer cumplir la ley, en el territorio que alberga los datos o incluso en un tercer país al mismo tiempo.

Debería tenerse en cuenta que muchos Estados pondrían objeciones – y algunos incluso lo considerarían un delito – si unas autoridades extranjeras encargadas de hacer cumplir la ley se dirigen directamente una persona que está físicamente presente en su territorio con el fin de solicitar su cooperación.

4. Declaración del T-CY

El T-CY está de acuerdo en que lo antedicho representa el entendimiento común de las Partes acerca del ámbito de aplicación y de los elementos del artículo 32.

Nota de orientación sobre el *spam*[51]

1. Introducción

En su 8ª sesión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió publicar unas Notas de orientación encaminadas a facilitar la utilización y la aplicación efectivas del Convenio sobre la ciberdelincuencia (Convenio de Budapest), también a la luz de las novedades jurídicas, políticas y tecnológicas.[52]

Las Notas de orientación representan el entendimiento común de las Partes en este tratado en lo que respecta a la utilización del Convenio.

En la presente Nota se aborda la cuestión del *spam*. El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras"[53]. Esto tiene por objeto asegurar que el Convenio abarque siempre las nuevas formas de *malware* o de delito.

Esta Nota de orientación muestra el modo en que diferentes artículos del Convenio se aplican al *spam*.

2. Disposiciones pertinentes del Convenio sobre la ciberdelincuencia (Convenio de Budapest) (CETS núm. 185)

El *spam* suele definirse como correo electrónico masivo no solicitado, en el que se envía un mensaje a un número considerable de direcciones de correo electrónico, y en el que la identidad personal del destinatario es irrelevante porque el mensaje está dirigido igualmente a muchos otros destinatarios sin distinción alguna.

Existen aspectos distintos en relación con:

- el contenido del *spam*,
- la acción de enviar *spam*, y
- el mecanismo utilizado para transmitir *spam*.

51. Adoptado por el T-CY en su 12ª sesión plenaria**.**
52. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
53. Párrafo 36 del Informe explicativo.

El contenido del *spam* puede ser lícito o no, y en los casos en que el contenido es ilícito (como ofertas de medicamentos falsos u ofertas financieras fraudulentas), el delito puede estar contemplado en la legislación nacional pertinente relativa a dichos delitos. La acción de transmitir *spam* (incluida la transmisión masiva de contenido inobjetable) puede ser un delito civil o penal en las jurisdicciones.

El Convenio no contempla el *spam* cuyo contenido no es ilícito y no causa interferencias en el funcionamiento de un sistema, pero que puede ser molesto para los destinatarios finales.

Las herramientas utilizadas para transmitir *spam* pueden ser ilícitas en virtud del Convenio de Budapest, y el *spam* se puede estar asociada con otros delitos no enumerados en la matriz que figura a continuación (véase, por ejemplo, el artículo 7).

Al igual que sucede con otras notas de orientación, cada disposición contiene una pauta que hace referencia a una intención ("ilegítima", "con una intención dolosa", etc.). En algunos casos de *spam*, esta intención puede ser difícil de demostrar.

3. Interpretación del T-CY de las disposiciones en las que se hace referencia al spam

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	El *spam* puede contener *malware* que puede acceder, o permitir el acceso, a un sistema informático.
Artículo 3 – Interceptación ilícita	El *spam* puede contener *malware* que puede interceptar ilícitamente las transmisiones de datos informáticos, o permitir su interceptación ilícita.
Artículo 4 – Ataques a la integridad de los datos	El *spam* puede contener *malware* que puede dañar, eliminar, deteriorar, alterar o suprimir datos informáticos.
Artículo 5 – Ataques a la integridad del sistema	La transmisión de *spam* puede socavar seriamente el funcionamiento de los sistemas informáticos. El *spam* puede contener *malware* que socave seriamente el funcionamiento de los sistemas informáticos.

Artículos pertinentes	Ejemplos
Artículo 6 – Abuso de los dispositivos	Los dispositivos definidos en el artículo 6 pueden utilizarse para la transmisión de *spam*. El *spam* puede contener dispositivos definidos en el artículo 6.
Artículo 8 – Falsificación informática	El *spam* puede utilizarse como dispositivo para la introducción, alteración, eliminación o supresión de datos informáticos, o para obstaculizar el funcionamiento de un sistema informático con el fin de obtener beneficios económicos ilícitos.
Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	El *spam* puede utilizarse para anunciar la venta de productos falsos, incluidos programas informáticos y otros artículos protegidos por derechos de propiedad intelectual.
Artículo 11 – Tentativa y complicidad	El *spam* y la transmisión de *spam* pueden utilizarse para procurar cometer varios delitos especificados en el tratado (por ejemplo, el artículo 7 sobre falsificación informática o el artículo 8 sobre fraude informático) o para ser cómplices de los mismos.
Artículo 13 – Sanciones y medidas	El *spam* puede tener múltiples objetivos delictivos, algunos de los cuales pueden tener serias repercusiones en las personas, o en las instituciones públicas o del sector privado. Aunque un Estado no penalice el *spam* en sí mismo, debería penalizar el comportamiento relacionado con el *spam*, como los delitos antedichos, y puede considerar circunstancias agravantes. En virtud del artículo 13, las Partes deberían asegurar que los delitos relacionados con el *spam* "estén sujetos a sanciones efectws, proporcionadas y disuasorias, incluidas penas privativas de libertad". Para las personas jurídicas esto puede comprender sanciones penales o no penales, incluidas sanciones monetarias.

4. Declaración del T-CY

La lista de artículos que figura anteriormente ilustra el uso delictivo multifuncional del *spam* y los delitos relacionados con el *spam*.

Por lo tanto, el T-CY está de acuerdo en que el Convenio de Budapest contempla estos aspectos del *spam*.

Nota de orientación sobre órdenes de presentación de datos relativos a los abonados (Artículo 18 del Convenio de Budapest)[54]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la Ciberdelincuencia (T-CY) decidió elaborar notas de orientación encaminadas a facilitar la utilización y aplicación efectivas del Convenio de Budapest sobre la Ciberdelincuencia, habida cuenta asimismo de las novedades jurídicas, políticas y tecnológicas.[55]

Aunque no son vinculantes, las notas de orientación representan el entendimiento común de las Partes en este tratado en lo que respecta a la utilización del Convenio.

En esta nota[56] se examina la cuestión de las órdenes de presentación de datos relativos a los abonados en virtud del artículo 18, a saber, las situaciones en las que:

- una persona a la que se ordena que comunique determinados datos informáticos está presente en el territorio de una Parte (artículo 18.1.a)),[57] y
- un proveedor de servicios al que se ordena que comunique datos relativos a los abonados ofrece sus servicios en el territorio de la Parte sin estar ubicado necesariamente en el territorio (artículo 18.1.b)).

Una nota orientativa sobre estos aspectos del artículo 18 es pertinente, habida cuenta de que:

- los datos relativos a los abonados es la información solicitada con más frecuencia en las investigaciones penales;
- el artículo 18 es una competencia interna;
- el crecimiento de la computación en la nube y del almacenamiento remoto de datos ha planteado una serie de dificultades a las autoridades competentes que tratan de acceder a determinados datos informáticos

54. Adoptada por el T-CY tras la 16ª reunión plenaria mediante procedimiento escrito (28 de febrero de 2017).
55. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
56. Esta nota de orientación se basa en la labor realizada por el Grupo sobre las Pruebas en la Nube del T-CY.
57. Es importante recordar que el artículo 18.i.a) del Convenio de Budapest no se limita a los datos relativos a los abonados, sino que también hace referencia a cualquier tipo de datos informáticos especificados. Sin embargo, en esta nota de orientación se aborda únicamente la presentación de datos relativos a los abonados.

– y, en particular, a los datos relativos a los abonados – con el fin de promover las investigaciones y enjuiciamientos penales;
– en la actualidad, las prácticas y procedimientos, al igual que las condiciones y salvaguardias para acceder a los datos relativos a los abonados, varían considerablemente entre las Partes en el Convenio, y
– es preciso responder a las preocupaciones relativas a la privacidad y a la protección de datos personales, a los fundamentos jurídicos de la jurisdicción referentes a los servicios ofrecidos en el territorio de una Parte sin que el proveedor de servicios esté establecido en dicho territorio, así como al acceso a los datos almacenados en jurisdicciones extranjeras o en lugares desconocidos o múltiples "dentro de la nube".

El servicio y la fuerza ejecutiva de las órdenes de presentación internas contra los proveedores establecidos fuera del territorio de una Parte plantean otras cuestiones que no se pueden abordar plenamente en una nota de orientación. Algunas Partes pueden exigir que los datos relativos a los abonados se soliciten a través de asistencia judicial mutua.

El artículo 18 es una medida que debe aplicarse en investigaciones y procedimientos penales específicos con arreglo al artículo 14 del Convenio de Budapest. Por consiguiente, las órdenes deben impartirse en casos concretos en lo que respecta a determinados abonados.

2. Artículo 18 del Convenio de Budapest

Texto de la disposición

Artículo 18 – Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y

b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

Extracto del Informe explicativo:

> 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 esta 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 están 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.[58]

¿Qué se entiende por "datos relativos a los abonados"?

La expresión "datos relativos a los abonados" se define en el artículo 18.3) del Convenio de Budapest:

> 3 A los efectos del presente artículo, se entenderá por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de

58. Párrafo 173 del Informe explicativo.

cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como 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 servicio;

c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

En el párrafo 177 del Informe explicativo se indica asimismo lo siguiente:

> 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.

La obtención de datos relativos a los abonados puede representar una injerencia menor en los derechos de las personas que la obtención de datos relativos al tráfico o al contenido.

¿Qué se entiende por "proveedor de servicios"?

El Convenio de Budapest sobre la Ciberdelincuencia aplica un concepto amplio de "proveedor de servicios", que se define en el artículo 1.c) del Convenio de Budapest.

A los efectos del presente Convenio:

c. por "proveedor de servicios" se entenderá:

i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

El artículo 18.1.b) debe aplicarse con respecto a cualquier proveedor de servicios que ofrezca sus servicios en el territorio de la Parte.[59]

3. Interpretación por el T-CY del artículo 18 del Convenio de Budapest en relación con los datos relativos a los abonados

El ámbito de aplicación del artículo 18.1.a)

- El ámbito de aplicación es amplio: una "persona" (que puede incluir un "proveedor de servicios") que esté presente en el territorio de la Parte.
- En lo que respecta a los datos informáticos, el ámbito de aplicación es amplio, pero no indiscriminado: cualesquiera datos informáticos "específicos" (motivo por el cual el artículo 18.1.a) no se limita a los "datos relativos a los abonados" y abarca todos los tipos de datos informáticos).
- Los datos informáticos específicos obran en poder de dicha persona o, si la persona no tiene posesión física de los mismos, dicha persona controla libremente los datos informáticos que deben presentarse con arreglo al artículo 18.1.a) desde dentro del territorio de la Parte.
- Los datos informáticos específicos se almacenan en sistema informático o en un dispositivo de almacenamiento de datos.
- La orden de presentación es impartida y ejecutada por las autoridades competentes en la Parte en la que se solicita y concede la orden.

El ámbito de aplicación del artículo 18.1.b)

El ámbito de aplicación del artículo 18.1.b) es más estrecho que el del artículo 18.1.a):

- El apartado b) se limita a un "proveedor de servicios".[60]
- El proveedor de servicios al que se imparte la orden no está necesariamente presente, pero ofrece sus servicios en el territorio de la Parte.
- Se limita a los "datos relativos a los abonados".

59. Los instrumentos de la Unión Europea establecen una distinción entre los proveedores de servicios de comunicación electrónica y los proveedores de servicios de la sociedad Internet. El concepto de "proveedor de servicios" plasmado en el artículo 1.c) del Convenio de Budapest abarca ambos.
60. El concepto de "persona" es más amplio que el de "proveedor de servicios", aunque "un proveedor de servicios" puede ser "una persona".

– Los datos relativos a los abonados hacen referencia a tales servicios y obran en poder o están bajo el control de dicho proveedor de servicios.

A diferencia del artículo 18.1.a), cuyo ámbito de aplicación se limita a las "personas presentes en el territorio de la Parte", el artículo 18.1.b) no hace referencia a cuestión de la ubicación del proveedor de servicios. Las Partes podrían aplicar la disposición en las circunstancias en las que el proveedor de servicios que ofrezca sus servicios en el territorio de la Parte no esté jurídica ni físicamente presente en el territorio.

3.1 Jurisdicción

El artículo 18.1.b) se limita a las circunstancias en las que la autoridad de la justicia penal que imparte la orden de presentación tiene jurisdicción respecto del delito en cuestión.

Esto puede incluir situaciones en las que el abonado es o era residente en dicho territorio, y está o estaba presente en el mismo, cuando se cometió el delito.

Esta interpretación del artículo 18 se entiende sin perjuicio de unas competencias más amplias o adicionales en el derecho interno de las Partes.

El acuerdo con la presente nota de orientación no conlleva la aprobación del servicio extraterritorial o del cumplimiento de una orden de presentación nacional impartida por otro Estado, y no crea nuevas obligaciones o relaciones entre las Partes.

3.2 ¿Cuáles son las características de una "orden de presentación"?

En virtud del artículo 18, una "orden de presentación" es una medida adoptada a nivel interno y debe preverse en el derecho penal interno. Una "orden de presentación" está limitada por la jurisdicción en materia judicial y de ejecución de la Parte en el que se concede la orden.

Con arreglo al artículo 18, las ordenes de presentación se refieren:

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.[61]

61. Párrafo 172 del Informe explicativo.

El Informe explicativo[62] del Convenio de Budapest se refiere a las órdenes de presentación como una medida flexible que es menos intrusiva que el registro o la incautación u otras medidas coercitivas, y en él se indica asimismo que:

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.

3.3 ¿Qué efectos tiene la ubicación de los datos?

El almacenamiento de los datos relativos a los abonados en otra jurisdicción no impide la aplicación del artículo 18 del Convenio de Budapest, siempre y cuando dichos datos obren en poder o estén bajo el control del proveedor de servicios. En el Informe explicativo se señala con respecto al:

- artículo 18.1.a), que "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 deban 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".[63]
- artículo 18.1.b), que "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 del almacenamiento de datos provista por otra compañía)."[64]

Por lo referente al artículo 18.1.b), una situación puede incluir un proveedor de servicios que tenga su sede en una jurisdicción, pero que almacene

62. Párrafo 171 del Informe explicativo.
63. Párrafo 173 del Informe explicativo. Con arreglo al artículo 18.1.a) del Convenio de Budapest, una "persona" puede ser una persona física o jurídica, incluido un proveedor de servicios.
64. Párrafo 173 del Informe explicativo.

los datos en otra jurisdicción. Los datos también pueden reproducirse en varias jurisdicciones o transferirse entre jurisdicciones, a discreción del proveedor de servicios y sin el conocimiento o el control del abonado. Los regímenes jurídicos reconocen cada vez más que, tanto en el ámbito de la justicia penal como en el ámbito de la privacidad y la protección de datos, la ubicación de los datos no es el factor determinante para establecer la jurisdicción.

3.4 ¿Qué se entiende por "ofreciendo sus servicios en el territorio de una Parte"?

El crecimiento de la computación en la nube ha planteado cuestiones en lo que respecta a cuando se considera que un proveedor de servicios esté ofreciendo sus servicios en el territorio de la Parte y, por lo tanto, se le pueda impartir una orden de presentación interna para que proporcione datos relativos a los abonados. Esto ha conducido a diversas interpretaciones por los tribunales en múltiples jurisdicciones en causas tanto civiles como penales.

Por lo referente al artículo 18.1.b), las Partes podrían considerar que un proveedor de servicios está "ofreciendo sus servicios en el territorio de la Parte", cuando:

- el proveedor de servicios permite a las personas que se encuentran en el territorio de la Parte abonarse a sus servicios[65] (y, por ejemplo, no bloquea el acceso a los mismos);

  y

- el proveedor de servicios ha establecido una conexión real y sustantiva con una Parte. Entre los factores pertinentes se cuentan la medida en que un proveedor de servicios orienta sus actividades a dichos abonados (por ejemplo, proporcionando publicidad local o publicidad en el idioma del territorio de la Parte), utiliza los datos relativos a los abonados (o datos relativos al tráfico conexos) en el curso de sus actividades, interactúa con los abonados en la Parte y pueda considerarse establecido en el territorio de una Parte.

El mero hecho de que un proveedor de servicios utilice un nombre de dominio o una dirección de correo electrónico que estén conectados con

65. Véase el párrafo 183 del Informe explicativo: "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."

un país determinado no crea una presunción de que su domicilio social esté establecido en dicho país. Por lo tanto, puede considerarse que se cumple el requisito de que los datos relativos a los abonados que deban presentarse hagan referencia a los servicios ofrecidos por un proveedor en el territorio de la Parte, aun cuando dichos servicios se ofrezcan a través de un nombre de dominio de primer nivel de código de país que se refiera a otra jurisdicción.

3.5 Consideraciones generales y salvaguardias

Se espera que las Partes en el Convenio formen una comunidad de confianza que respete el artículo 15 del Convenio de Budapest.

> Artículo 15 – Condiciones y salvaguardias
>
> 1 – Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.
>
> 2 – Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.
>
> 3 – Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

3.6. La aplicación del artículo 18 con respecto a los datos relativos a los abonados

Por consiguiente, la presentación de datos relativos a los abonados en virtud del artículo 18 del Convenio de Budapest podría ordenarse si se cumplen los siguientes criterios en una investigación penal específica y por lo referente a determinados abonados:

<table>
<tr><td colspan="3">SI
La autoridad de la justicia penal tiene jurisdicción respecto del delito en cuestión;</td></tr>
<tr><td colspan="3">Y SI
los datos relativos a los abonados obran en poder o están bajo el control del proveedor de servicios;</td></tr>
<tr><td colspan="3">Y SI</td></tr>
<tr><td>Artículo 18.1.a)
La persona (proveedor de servicios) se encuentra en el territorio de la Parte.</td><td>O</td><td>Artículo 18.1.b)
Una Parte considera que un proveedor de servicios está “ofreciendo sus servicios en el territorio de la Parte” cuando, por ejemplo:
– el proveedor de servicios permite a las personas que se encuentran en el territorio de la Parte abonarse a sus servicios (y, por ejemplo, no bloquea el acceso a los mismos);
y
– el proveedor de servicios ha establecido una conexión real y sustantiva con una Parte. Entre los factores pertinentes se cuentan la medida en que un proveedor de servicios orienta sus actividades a dichos abonados (por ejemplo, proporcionando publicidad local o publicidad en el idioma del territorio de la Parte), utiliza los datos relativos a los abonados (o datos relativos al tráfico conexos) en el curso de sus actividades, interactúa con los abonados en la Parte y pueda considerarse establecido en el territorio de una Parte.</td></tr>
<tr><td colspan="3">Y SI</td></tr>
<tr><td></td><td></td><td>- los datos relativos a los abonados que deben presentarse hacen referencia a los servicios ofrecidos por un proveedor en el territorio de la Parte.</td></tr>
</table>

4. Declaración del T-CY

El T-CY está de acuerdo en que lo mencionado anteriormente representa el entendimiento común de las Partes en cuanto al ámbito de aplicación y los elementos del artículo 18 del Convenio de Budapest con respecto a la presentación de datos relativos a los abonados.

Nota de orientación sobre el terrorismo[66]

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la Ciberdelincuencia (T-CY) decidió elaborar notas de orientación encaminadas a facilitar la utilización y aplicación efectivas del Convenio de Budapest sobre la Ciberdelincuencia, habida cuenta asimismo de la evolución del derecho, la política y la tecnología.[67]

Las notas de orientación representan el entendimiento común de las Partes en este tratado en lo que respecta a la utilización del Convenio.

En la presente nota se examina el modo en que diferentes artículos del Convenio podrían aplicarse al terrorismo.

Muchos países son Partes en numerosos tratados, y objeto de resoluciones del Consejo de Seguridad de las Naciones Unidas, que exigen la penalización de diferentes formas de terrorismo, de la facilitación del terrorismo, del apoyo al terrorismo y de los actos preparatorios de terrorismo. En los casos de terrorismo, los países suelen apoyarse en delitos derivados de esos tratados que se centran en temas concretos, y en otros delitos contemplados en la legislación nacional.

El Convenio de Budapest no es un tratado que verse específicamente sobre el terrorismo. Sin embargo, los delitos sustantivos previstos por el Convenio pueden cometerse como actos de terrorismo, para facilitar el terrorismo y apoyar el terrorismo, también financieramente, o como actos preparatorios de terrorismo.

Además, los instrumentos procesales y de asistencia judicial mutua internacional contemplados en el Convenio están disponibles para las investigaciones y enjuiciamientos de delitos de terrorismo y relacionados con el terrorismo.

El ámbito de aplicación y los límites se definen en los artículos 14,2) y 25,1) del Convenio de Budapest:

> Artículo 14,2)
>
> 2 Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:
>
> a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
>
> b. a cualquier otro delito cometido por medio de un sistema informático; y

66. Adoptado por el T-CY en su 16ª sesión plenaria (14-15 noviembre 2016).
67. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).

c. a la obtención de pruebas electrónicas de cualquier delito.

Artículo 25,1)

Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

Véanse asimismo los artículos 23 y 27,1) del Convenio de Budapest, así como otras notas de orientación, tales como las notas de orientación sobre los ataques graves a la integridad de la infraestructura o los ataques de denegación de servicio distribuido.

2. Disposiciones pertinentes del Convenio de Budapest sobre la Ciberdelincuencia (STE núm. 185)

2.1 Disposiciones de procedimiento

Las facultades procesales previstas por el Convenio (artículos 14 a 21) pueden utilizarse en una investigación o procedimiento penal específico en cualquier tipo de caso, tal como dispone el artículo 14.

De hecho, las medidas procesales específicas pueden ser muy útiles, por ejemplo en los casos de terrorismo, si se utilizó un sistema informático para cometer o facilitar el delito, o si existen pruebas electrónicas de dicho delito, o si puede identificarse a un sospechoso a través de los datos relativos a los abonados, incluida una dirección del protocolo de Internet (IP). Así pues, en los casos de terrorismo, las Partes pueden recurrir a la conservación rápida de datos informáticos almacenados, las órdenes de presentación, el registro y la confiscación de datos informáticos almacenados, y otros instrumentos con el fin de obtener pruebas electrónicas en investigaciones y enjuiciamientos de delitos de terrorismo y relacionados con el terrorismo en el ámbito de aplicación señalado anteriormente.

2.2 Disposiciones sobre la asistencia judicial mutua internacional

Los poderes en materia de cooperación internacional previstos por el Convenio (artículos 23 a 35) tienen un alcance similar.

Así pues, las Partes deben poner a disposición la conservación rápida de datos informáticos almacenados, las órdenes de presentación, el registro y la confiscación de datos informáticos almacenados, y otros instrumentos, así

como otras disposiciones en materia de cooperación internacional, a fin de concertar esfuerzos con otras Partes en las investigaciones y enjuiciamientos de delitos de terrorismo y relacionados con el terrorismo en el ámbito de aplicación señalado anteriormente.

2.3 Disposiciones sustantivas del derecho penal

Por último, tal como se ha señalado anteriormente, los terroristas y los grupos terroristas, como parte de la consecución de sus objetivos, pueden cometer actos tipificados como delito en el Convenio.

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	Se puede acceder ilícitamente a un sistema informático con el fin de obtener información de identificación personal (p.ej., información sobre funcionarios gubernamentales con el fin de seleccionarlos específicamente como objetivo de ataque).
Artículo 3 – Interceptación ilícita	Pueden interceptarse ilícitamente transmisiones no públicas de datos informáticos hasta, desde o dentro de un sistema informático, con el fin de obtener información sobre la localización de una persona (p.ej., para dirigir específicamente un ataque contra ella)
Artículo 4 – Ataques a la integridad de los datos	Los datos informáticos pueden dañarse, eliminarse, deteriorarse, modificarse o suprimirse (p.ej., los expedientes médicos de un hospital pueden modificarse para que sean peligrosamente incorrectos, o una interferencia con el sistema de control del tráfico aéreo puede afectar a la seguridad de los vuelos).
Artículo 5 – Ataques a la integridad del sistema	El funcionamiento de un sistema informático puede obstaculizarse con fines terroristas (p.ej., obstaculización del sistema en el que se almacenan registros de la Bolsa de valores, que puede dar lugar a que éstos sean inexactos, u obstaculización del funcionamiento de infraestructura esencial).
Artículo 6 – Abuso de los dispositivos	La venta, adquisición para su utilización, importación, distribución u otros actos que pongan a disposición contraseñas informáticas, códigos de acceso o datos similares que permiten el acceso a sistemas informáticos pueden facilitar un atentado terrorista (p.ej., pueden causar daños en la red eléctrica de un país).

Artículos pertinentes	Ejemplos
Artículo 7 – Falsificación informática	Los datos informáticos (p.ej., los utilizados en los pasaportes electrónicos) pueden introducirse, modificarse, eliminarse o suprimirse, dando lugar a que se tomen en consideración datos falsos y a que se actúe sobre la base de los mismos con fines legales como si fueran auténticos.
Artículo 8 – Fraude informático	Los datos informáticos pueden introducirse, modificarse, eliminarse o suprimirse, y/o puede atentarse contra la integridad de un sistema informático, dando lugar a que algunas personas pierdan bienes (p.ej., un ataque al sistema bancario de un país puede causar la pérdida de bienes a una serie de víctimas).
Artículo 11 – Tentativa y complicidad	Los delitos especificados en el tratado pueden conducir a tentativa o complicidad con fines terroristas.
Artículo 12 – Responsabilidad de las personas jurídicas	Los delitos contemplados en los artículos 2 a 11 del Convenio en apoyo del terrorismo pueden ser cometidos por personas jurídicas que serían responsables en virtud del artículo 12.
Artículo 13 – Sanciones	Los delitos cubiertos por el Convenio pueden suponer una amenaza para las personas y la sociedad, en particular cuando están dirigidos a sistemas que son fundamentales en la vida cotidiana, tales como el transporte público, los sistemas bancarios o la infraestructura hospitalaria. Los efectos pueden variar entre los diferentes países, dependiendo asimismo de su grado de interconexión y de su dependencia de dichos sistemas. Una Parte puede prever en su legislación nacional una sanción que sea inadecuadamente indulgente con los actos relacionados con el terrorismo en relación con los artículos 2 a 11, y puede no permitir la consideración de circunstancias agravantes o de la tentativa y complicidad. Esto puede significar que las Partes deben considerar enmiendas a su legislación nacional. En virtud del artículo 13, las Partes deberán asegurar que los delitos relacionados con dichos actos "estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad".

Artículos pertinentes	Ejemplos
	Las Partes también pueden considerar circunstancias agravantes, por ejemplo, si dichos actos afectan a un gran número de sistemas o causan daños considerables, con inclusión de muertes o lesiones físicas, o daños a infraestructura esencial.

Otros delitos cubiertos por el Convenio, pero que no se han mencionado de manera específica anteriormente, incluida la producción de materiales destinados a la explotación de los niños o el tráfico de propiedad intelectual robada, también pueden cometerse en relación con el terrorismo.

Para las Partes en el Convenio de Budapest que también son Partes en el Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, (STE núm. 189)[68], dos artículos del Protocolo son pertinentes, ya que pueden hacer referencia a la radicalización y al extremismo violento que pueden conducir al terrorismo, a saber, el artículo 4, relativo a las amenazas con motivación racista y xenófoba, y el artículo 6, referente a la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

3. Declaración del T-CY

El T-CY está de acuerdo en que los delitos sustantivos contemplados en el Convenio pueden ser asimismo actos de terrorismo tal como se definen en la legislación aplicable.

Los delitos sustantivos cubiertos por el Convenio pueden cometerse con objeto de facilitar el terrorismo y apoyar el terrorismo, también financieramente, o como actos preparatorios de terrorismo.

Los instrumentos procesales y de asistencia judicial mutua internacional previstos por el Convenio pueden utilizarse con miras a investigar el terrorismo, su facilitación, el apoyo al mismo, o los actos preparatorios de terrorismo.

68. Véase el sitio web: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Nota de orientación sobre aspectos de la injerencia en los procesos electorales por medio de sistemas informáticos contemplados en el Convenio de Budapest[69]

Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la Ciberdelincuencia

(T-CY) decidió elaborar notas de orientación encaminadas a facilitar la utilización y aplicación efectivas del Convenio de Budapest sobre la Ciberdelincuencia, habida cuenta asimismo de los avances jurídicos, políticos y tecnológicos.[70]

Aunque no son vinculantes, las notas de orientación representan el entendimiento común de las Partes en este tratado en lo que respecta a la utilización del Convenio.

La injerencia en los procesos electorales a través de actividades cibernéticas maliciosas contra las computadoras y los datos utilizados en los procesos y campañas electorales socava los procesos electorales libres, justos y limpios, así como la confianza en la democracia. Las operaciones de desinformación, como se experimenta en particular desde 2016, pueden utilizar actividades cibernéticas maliciosas y tener el mismo efecto. Tal vez sea necesario adaptar los procesos electorales nacionales a las realidades de la sociedad de la información, y los sistemas informáticos utilizados en los procesos electorales y las campañas conexas deben hacerse más seguros.

En este contexto, es preciso intensificar los esfuerzos para sancionar dicha injerencia cuando constituye un delito: una respuesta eficaz de la justicia penal puede desalentar la injerencia en los procesos electorales y tranquilizar al electorado en lo que respecta al uso de las tecnologías de la información y de las comunicaciones en dichos procesos.

En la presente Nota se examina la manera en que los artículos del Convenio pueden aplicarse a aspectos de la injerencia en los procesos electorales por medio de sistemas informáticos.

69. Adoptada por el T-CY tras la 21ª reunión plenaria (8 de julio de 2019).
70. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).

Los delitos sustantivos contemplados en el Convenio pueden cometerse como actos de injerencia en los procesos electorales o como actos preparatorios que facilitan dicha injerencia.

Además, los instrumentos procesales nacionales y los instrumentos internacionales de asistencia jurídica en materia penal mencionados en el Convenio están disponibles para las investigaciones y acciones judiciales relacionadas con la injerencia en los procesos electorales. El alcance y los límites de los poderes procesales y de los instrumentos para la cooperación internacional se definen en los artículos 14.2 y 25.1 del Convenio de Budapest:

> Artículo 14.2
>
> 2 Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:
>
> a los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;
>
> b otros delitos cometidos por medio de un sistema informático; y
>
> c la obtención de pruebas electrónicas de un delito.
>
> Artículo 25.1
>
> Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

Los poderes procesales previstos en el Convenio están sujetos a las condiciones y salvaguardias establecidas en el artículo 15.

Disposiciones pertinentes del Convenio de Budapest sobre la Ciberdelincuencia (STE núm. 185)

Disposiciones procesales

Los poderes procesales previstos en el Convenio (artículos 14 a 21) pueden utilizarse para fines de investigaciones o procedimientos penales específicos en cualquier tipo de injerencia en los procesos electorales, tal como prevé el artículo 14.

Las medidas de procedimiento específicas pueden ser muy útiles en las investigaciones penales de la injerencia en los procesos electorales. Por ejemplo,

en los casos de injerencia en los procesos electorales, puede utilizarse un sistema informático para cometer o facilitar un delito, las pruebas de dicho delito pueden almacenarse en formato electrónico, o puede identificarse a un sospechoso a través de la información sobre los abonados, incluida una dirección de protocolo de Internet. De manera análoga, la financiación política ilegal puede detectarse por medio de correos electrónicos conservados; las comunicaciones de voz entre los conspiradores pueden captarse de acuerdo con la interceptación debidamente autorizada, y la utilización ilícita de datos puede mostrarse por huellas electrónicas.

Así pues, en las investigaciones penales de la injerencia en los procesos electorales, las Partes pueden utilizar la conservación rápida de datos informáticos almacenados, las órdenes de presentación, el registro y la confiscación de datos informáticos almacenados, y otras herramientas para recabar las pruebas electrónicas necesarias para la investigación y la persecución de tales delitos relacionados con la injerencia en los procesos electorales.

Disposiciones sobre la asistencia judicial internacional en materia penal

Las poderes en materia de cooperación internacional previstos en el Convenio (artículos 23 a 35) tienen un alcance similar y pueden ayudar a las Partes en las investigaciones de la injerencia en los procesos electorales.

Así pues, las Partes deberán proporcionar disposiciones sobre la conservación rápida de datos informáticos almacenados, las órdenes de presentación, el registro y la confiscación de datos informáticos almacenados, así como otras disposiciones relativas a la cooperación internacional.

Disposiciones sobre el derecho penal sustantivo

Por último, como se ha señalado anteriormente, la injerencia en los procesos electorales puede conllevar los siguientes tipos de conducta, cuando tienen lugar sin derecho, tipificados como delitos por el Convenio sobre la Ciberdelincuencia. El T-CY pone de relieve que los ejemplos que figuran a continuación sólo son ejemplos – es decir, dado que la injerencia en los procesos electorales es un fenómeno que está desarrollándose, puede aparecer en muchas formas no mencionadas a continuación. Sin embargo, el T-CY espera que el Convenio sobre la Ciberdelincuencia sea suficientemente flexible para abordarlas.

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	Puede que se acceda ilícitamente a un sistema informático a fin de obtener información sensible o confidencial relacionada con los candidatos, las campañas, los partidos políticos o los votantes.
Artículo 3 – Interceptación ilícita	Puede que se intercepten de manera ilícita las transmisiones no públicas de datos informáticos efectuadas a, o desde, un sistema informático, a fin de obtener información sensible o confidencial relacionada con los candidatos, las campañas, los partidos políticos o los votantes.
Artículo 4 – Injerencia en los datos	Puede que se dañen, borren, deterioren, alteren o supriman datos informáticos para modificar sitios web, alterar las bases de datos de los votantes, o manipular los resultados de los votos, por ejemplo, manipulando los dispositivos de voto.
Artículo 5 – Injerencia en el sistema	Puede que se obstaculice el funcionamiento de los sistemas informáticos utilizados en los procesos o campañas electorales para interferir en la transmisión de mensajes durante las campañas, dificultar la inscripción de votantes, inhabilitar la emisión de votos o impedir el recuento de votos a través de la denegación de ataques de servicio, programas maliciosos u otros medios.
Artículo 6 – Abuso de los dispositivos	La venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de contraseñas de computadora, códigos de acceso o datos similares que permiten acceder a sistemas informáticos pueden facilitar la injerencia en los procesos electorales, como el robo de datos sensibles de los candidatos políticos, los partidos o las campañas.
Artículo 7 – Falsificación informática	Puede que se introduzcan, alteren, borren o supriman datos informáticos (por ejemplo, los datos utilizados en las bases de datos de los votantes), de tal manera que datos no auténticos sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos. Por ejemplo, algunos países exigen que las campañas electorales hagan públicos los estados financieros. La falsificación de datos

	informáticos podría dar la impresión de que el estado financiero es incorrecto o de que se ocultan fuentes cuestionables de fondos para la campaña.
Artículo 11 – Tentativa y complicidad	Puede haber una tentativa de comisión de los delitos especificados en el tratado, o una complicidad con este fin, en apoyo de la injerencia en los procesos electorales.
Artículo 12 – Responsabilidad de las personas jurídicas	Puede que los delitos contemplados en los artículos 2 a 11 del Convenio en apoyo de la injerencia en los procesos electorales sean realizados por personas jurídicas que serían responsables en virtud del artículo 12.
Artículo 13 – Sanciones	Los delitos cubiertos por el Convenio pueden suponer una amenaza para las personas y la sociedad, en particular cuando atentan contra aspectos fundamentales de la vida política, como los procesos electorales. Las acciones delictivas y sus efectos pueden variar de un país a otro, pero la injerencia en los procesos electorales puede socavar la confianza en los procesos democráticos, cambiar el resultado de un proceso electoral, exigir el gasto y la agitación que conlleva un segundo proceso electoral, o causar violencia física entre los partidarios de los procesos electorales y las comunidades. Puede que una Parte prevea en su legislación nacional una sanción que es indebidamente indulgente para los actos relacionados con los procesos electorales en relación con los artículos 2 a 11, y tal vez no permita la consideración de circunstancias agravantes o de la tentativa y la complicidad. Esto puede significar que las Partes deben considerar la introducción de enmiendas en su legislación nacional. Las Partes deberían garantizar, en virtud del artículo 13, que los delitos relacionados con tales actos puedan dar lugar a "la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Las Partes también pueden considerar circunstancias agravantes, por ejemplo, si tales actos afectan en gran medida un proceso electoral o causan muertes o lesiones físicas o considerables daños materiales.

Declaración del T-CY

El T-CY está de acuerdo en que los delitos sustantivos contemplados en el Convenio también pueden ser actos de injerencia en los procesos electorales tal como se define en la legislación aplicable, es decir, delitos contra unos procesos electorales libres, justos y limpios.

Los delitos sustantivos cubiertos por el Convenio pueden cometerse para facilitar o preparar actos de injerencia en los procesos electorales, o para participar en dichos actos.

Los instrumentos procesales y de asistencia judicial en materia penal especificados en el Convenio pueden utilizarse para investigar la injerencia en los procesos electorales, su facilitación, su participación en los mismos, o los actos preparatorios.

Nota de orientación sobre aspectos del ransomware cubiertos por el Convenio de Budapest

Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la Delincuencia (TCY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la Ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[71]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

Durante décadas, los delincuentes han cometido diferentes formas de ciberdelincuencia para extorsionar a organizaciones y particulares. Por ejemplo, el robo y posterior amenaza de divulgación pública de datos personales u otra información sensible para coaccionar el pago de un rescate sigue siendo una práctica frecuente. Sin embargo, en la última década han surgido formas más complejas de ransomware y delitos conexos. Estas consisten en el cifrado de datos o sistemas informáticos, con el consiguiente bloqueo de los usuarios, y las posteriores peticiones de rescate a cambio de la (promesa de) restauración del acceso. Los delincuentes también pueden amenazar con divulgar información sensible o personal, en un intento de obtener más eficazmente los pagos de las víctimas.

Estos delitos de ransomware son posibles gracias a que la tecnología permite lo siguiente:

- cifrado sólido de los datos o sistemas informáticos de las víctimas;
- uso de sistemas de comunicación difíciles de rastrear para enviar las peticiones de pago de rescate, así como las herramientas de descifrado;
- pago del rescate de forma difícil de rastrear, como por ejemplo a través de monedas virtuales que son más fáciles de ocultar que las monedas fiduciarias tradicionales.

Los ataques "WannaCry" y "NotPetya" de 2016 y 2017 afectaron a ordenadores y atrajeron gran atención en todo el mundo. La pandemia de COVID-19, surgida en 2020, conllevó que las sociedades dependieran en mayor medida de las tecnologías de la información y la comunicación, lo que aumentó las

71. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).

oportunidades de explotación con fines delictivos. Esto contribuyó a un nuevo aumento de los delitos de ransomware. Se tiene constancia de que ataques contra los sistemas informáticos de hospitales han provocado la muerte de pacientes. Además, los delitos de ransomware contra infraestructuras críticas provocaron que se declarara una situación de emergencia nacional en Costa Rica en abril de 2022. El uso de ransomware se considera ahora una forma grave de ciberdelincuencia que está afectando a intereses esenciales de individuos, empresas, sociedades y Gobiernos.

Por ello, el T-CY, en su 26ª reunión plenaria (10 y 11 de mayo de 2022), decidió elaborar una nota de orientación para mostrar cómo se tipifican los aspectos de los delitos de ransomware en las disposiciones de derecho penal sustantivo del Convenio sobre la Ciberdelincuencia y cómo se pueden utilizar las facultades procesales y las disposiciones en materia de cooperación internacional de este tratado para investigar y perseguir los delitos de ransomware y cooperar para hacerles frente.

Las presentes notas de orientación también hacen referencia al Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia (STCE 224) que proporcionará herramientas adicionales para favorecer la "cooperación reforzada y la divulgación de pruebas electrónicas" a las Partes de este Protocolo una vez que entre en vigor.

Las notas de orientación anteriores del T-CY relativas a programas informáticos malintencionados (malware), botnets, usurpación de identidad y ataques graves a la integridad de infraestructuras siguen siendo pertinentes también en lo que respecta a los delitos de ransomware.

Delitos de ransomware

El ransomware es un tipo de malware diseñado para impedir, mediante cifrado, que un usuario pueda acceder a sus datos y sistemas informáticos. A continuación, se pide al usuario objetivo que pague un rescate a cambio de la (promesa de) restauración de dicho acceso.

Los delitos de ransomware suelen implicar:

1. Actos preparatorios, por ejemplo:
   - la producción, venta, obtención o cualquier otra forma de puesta a disposición del ransomware, es decir, de un «dispositivo» según se contempla en el artículo 6 del Convenio sobre la Ciberdelincuencia;

- la producción, venta, obtención o cualquier otra forma de puesta a disposición de otros dispositivos según se contempla en el artículo 6 que se utilicen en la preparación de delitos de ransomware, como malware para obtener acceso no autorizado a los sistemas de las víctimas, o botnets para distribuir ransomware;
- la obtención de listas de correo u otra información pertinente sobre los objetivos. Algunos de estos actos preparatorios pueden constituir en sí mismos delitos o considerarse un tipo de tentativa y complicidad en la comisión de delitos de ransomware, como la exfiltración de bases de datos mediante registradores de teclado, el uso de botnets o la usurpación de identidad[72].

2. La distribución o instalación de ransomware, por ejemplo:

- mediante correos electrónicos con archivos adjuntos que contengan el malware o dirigidos a usuarios de aplicaciones de mensajería con enlaces incrustados en los mensajes. La incitación a los usuarios para que accedan a dichos archivos adjuntos o enlaces —y, por tanto, para que instalen el malware— puede facilitarse además mediante ingeniería social u otras técnicas de usurpación de identidad;
- mediante el acceso remoto a un sistema informático.

3. Cifrado del sistema informático, o de partes de este, o de datos mediante el ransomware, con lo que se impide al usuario acceder a los datos o al sistema o hacer uso de ellos de cualquier otro modo.

4. Solicitud, obtención y transferencia del pago del rescate, por ejemplo:

- la solicitud del rescate a cambio de (la promesa de) restablecer el acceso a los datos o al sistema, lo que equivale a extorsión o chantaje, pero posiblemente también a otros delitos;
- la comunicación entre el delincuente y el objetivo a través de medios de comunicación difíciles de rastrear, incluido el uso de la red TOR. Las herramientas de descifrado también pueden comunicarse de esta manera;
- la obtención del rescate de un modo que sea difícil de rastrear, normalmente en forma de criptomoneda, a lo que a menudo sigue el blanqueo de los productos del delito para ocultar aún más la identidad del autor y las ganancias.

72. Véanse las notas de orientación (coe.int) pertinentes.

Desde 2021, el mercado del ransomware está cada vez más organizado y profesionalizado, y ofrece un modelo de negocio que se suele denominar ransomware como servicio (o RaaS) para cometer delitos de ransomware. Este modelo de negocio ha llevado a los ciberdelincuentes a utilizar servicios independientes para negociar pagos y ayudar a las víctimas a realizar estos últimos. Asimismo, algunos servicios ofrecen un centro de ayuda las 24 horas del día para agilizar el pago de los rescates y ayudar a restaurar los sistemas o datos cifrados.

Disposiciones pertinentes del Convenio sobre la Ciberdelincuencia (STE 185)

Penalización de los delitos relacionados con el ransomware

En virtud del Convenio sobre la Ciberdelincuencia, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de determinados actos. Los siguientes artículos y los delitos correspondientes previstos en la legislación nacional de las Partes que aplican el Convenio pueden ser pertinentes para las investigaciones y los procedimientos penales relativos a los delitos de ransomware.

Artículos pertinentes	Ejemplos
Artículo 2 – Acceso ilícito	Los delitos de ransomware implican el acceso ilícito a un sistema informático de una víctima y, por lo tanto, un delito según el artículo 2.
Artículo 3 – Interceptación ilícita	Las variantes de ransomware pueden incluir medios para interceptar transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo. La obtención de información sobre objetivos o de credenciales de acceso también se puede considerar como delito de interceptación ilícita.
Artículo 4 – Ataques a la integridad de los datos	El ransomware está diseñado específicamente con el fin de interferir en los datos informáticos y, por tanto, su uso constituye un delito según el artículo 4.
Artículo 5 – Ataques a la integridad del sistema	El ransomware puede estar diseñado con el fin de interferir en el funcionamiento de un sistema informático y su uso es, por tanto, un delito según el artículo 5.

Artículo 6 – Abuso de los dispositivos	El ransomware es un tipo de malware y, por tanto, un dispositivo "concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5". Así, la "producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición" de ransomware constituyen un delito según el artículo 6.
Artículo 7 – Falsificación informática	Con el fin de obtener acceso ilícito a los sistemas de las víctimas, los autores de los ataques de ransomware utilizan a menudo la suplantación de identidad (phishing) y otras técnicas de ingeniería social, lo que en ciertos casos puede constituir una falsificación informática, es decir, la generación de datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como si fuesen auténticos.
Artículo 8 – Fraude informático	Los delitos de ransomware causan un perjuicio patrimonial, ya que interfieren en los datos informáticos o en el funcionamiento de un sistema informático con intención fraudulenta o dolosa de obtener, de manera ilegítima, un beneficio económico.
Artículo 11 – Tentativa y complicidad	Los delitos especificados en el tratado pueden ser la tentativa o complicidad en la comisión de delitos relacionados con el ransomware. Diferentes personas pueden estar implicadas, por ejemplo, en la producción, obtención o puesta a disposición de otro modo de ransomware, o en la obtención de información sobre objetivos.
Artículo 12 – Responsabilidad de las personas jurídicas	Los delitos de ransomware contemplados en los artículos 2 a 11 del Convenio descritos anteriormente pueden ser cometidos por personas jurídicas que serían responsables en virtud del artículo 12.

Artículo 13 – Sanciones	Los delitos relacionados con el ransomware contemplados en el Convenio pueden suponer una amenaza significativa para las personas y para la sociedad, especialmente cuando los delitos se dirigen contra infraestructuras críticas de información y causan un riesgo significativo para la vida o la seguridad de cualquier persona física. Por lo tanto, las Partes deben asegurar, de conformidad con el artículo 13, que los delitos relacionados con tales actos puedan dar lugar a "la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad". Esto asegura que, en virtud de su legislación nacional, las sanciones disponibles sean apropiadas dada la amenaza que supone el ransomware y tengan en cuenta toda la gama de responsabilidades penales, también sobre la base de la tentativa y complicidad en la comisión de una actividad delictiva. Asimismo, las Partes pueden considerar la posibilidad de aplicar sanciones más severas cuando concurran circunstancias agravantes, por ejemplo, si tales actos afectan de forma significativa al funcionamiento de infraestructuras críticas o causan la muerte o lesiones físicas a una persona física o daños materiales significativos.

Por lo tanto, los delitos de ransomware pueden comprender conductas que deben penalizarse de conformidad con los artículos 2 a 8, así como con el artículo 11 (tentativa y complicidad), y que también pueden conllevar que se exija responsabilidad a las personas jurídicas en virtud del artículo 12 del Convenio sobre la Ciberdelincuencia.

Las actividades de ransomware pueden comprender una amplia gama de otros delitos en virtud de la legislación penal nacional.

Disposiciones sobre procedimiento

En virtud del Convenio sobre la Ciberdelincuencia, "[c]ada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a" adoptar determinadas medidas procesales para investigar los delitos de conformidad con los artículos 2 a 11 del Convenio y para obtener pruebas en formato electrónico (véase el artículo 14 del Convenio). Dichas medidas también se podrán utilizar para las investigaciones y los procedimientos penales relacionados con los delitos de ransomware.

Artículos pertinentes	Ejemplos
Artículo 14 – Ámbito de aplicación de las disposiciones sobre procedimiento	Las facultades procesales del Convenio (artículos 16 a 21) se podrán utilizar en una investigación o procedimiento penal específicos no solo con respecto a los delitos mencionados anteriormente en virtud del Convenio, sino también con respecto a la obtención de pruebas en formato electrónico de cualquier otro delito relacionado con el ransomware, tal como se defina en el derecho interno de una Parte.
Artículo 15 – Condiciones y salvaguardias	Estas condiciones y salvaguardias también se aplican a las investigaciones y procedimientos penales relacionados con los delitos de ransomware.
Artículo 16 – Conservación rápida de datos informáticos almacenados	Esta facultad se podrá utilizar para conservar rápidamente los datos informáticos almacenados relacionados con delitos de ransomware, incluidos, por ejemplo, los datos sobre el origen o la vía de distribución del ransomware o de las comunicaciones en las que se solicite un rescate o se faciliten herramientas de descifrado, si procede. Esta facultad también se podrá utilizar para adoptar las medidas que sean necesarias para la conservación de otros datos relacionados con delitos de ransomware, como las comunicaciones entre sospechosos o datos almacenados por sospechosos que puedan constituir pruebas de tales delitos.
Artículo 17 – Conservación y revelación parcial rápidas de los datos sobre el tráfico	Esta facultad se podrá utilizar para obtener rápidamente una cantidad suficiente de datos sobre el tráfico con el fin de identificar a otros proveedores de servicios y la vía a través de la cual se transmitieron las comunicaciones relacionadas con los delitos de ransomware.
Artículo 18 – Orden de presentación	Las órdenes de presentación previstas en el artículo 18 se pueden utilizar para ordenar a una persona que presente datos informáticos almacenados relacionados con delitos de ransomware. Puede tratarse de proveedores de servicios, instituciones financieras, incluidos proveedores de servicios y plataformas de activos virtuales, así como otras personas físicas o jurídicas. Estas órdenes son vitales para obtener, por ejemplo, información de los abonados de los proveedores relacionada con cuentas e infraestructuras asociadas al ransomware.

Artículo 19 – Registro y confiscación de datos informáticos almacenados	Las disposiciones sobre registro y confiscación previstas en el artículo 19 se pueden utilizar para registrar y confiscar datos informáticos almacenados relacionados con delitos de ransomware.
Artículo 20 – Obtención en tiempo real de datos sobre el tráfico	Las facultades previstas en el artículo 20 se podrán utilizar para obtener en tiempo real datos sobre el tráfico relacionados con delitos de ransomware.
Artículo 21 – Interceptación de datos sobre el contenido	Las facultades previstas en el artículo 21 se podrán utilizar para interceptar determinados datos sobre el contenido relacionados con delitos de ransomware, como, por ejemplo, las comunicaciones entre sospechosos.

Por tanto, en las investigaciones o procedimientos penales relacionados con delitos de ransomware, las Partes podrán utilizar la conservación rápida de datos informáticos almacenados, las órdenes de presentación, el registro y confiscación de datos informáticos almacenados, así como otras herramientas para obtener pruebas electrónicas.

Disposiciones en materia de cooperación internacional

Artículos pertinentes	Ejemplos
Principios y procedimientos generales relativos a la cooperación internacional de los artículos 23 a 28	Los principios y procedimientos generales relativos a la cooperación internacional de los artículos 23 a 28 del Convenio —es decir, sobre extradición y asistencia mutua, entre otros— también son aplicables a los delitos relacionados con el ransomware. El artículo 26 puede ser especialmente útil en la medida en que una Parte que posea información valiosa sobre delitos de ransomware obtenida mediante investigaciones propias puede, dentro de los límites de su derecho interno, transmitir dicha información a la otra Parte sin que medie una solicitud previa (véase el párrafo 260 del Informe explicativo del Convenio sobre la Ciberdelincuencia). Según el artículo 23 y el artículo 25.1, las Partes en el Convenio deben cooperar entre sí, de conformidad con las disposiciones de los artículos 23 a 28, "para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos" y para "la obtención de pruebas electrónicas de los delitos".

Disposiciones específicas sobre cooperación internacional de los artículos 29 a 35.	Las disposiciones específicas del capítulo III del Convenio se pueden utilizar para la cooperación internacional y la obtención de pruebas relacionadas con los delitos de ransomware: – Artículo 29 – Conservación rápida de datos informáticos almacenados – Artículo 30 – Revelación rápida de datos conservados sobre el tráfico – Artículo 31 – Asistencia mutua en relación con el acceso a datos informáticos almacenados – Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público – Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico – Artículo 34 – Asistencia mutua en relación con la interceptación de datos sobre el contenido – Artículo 35 – Red 24/7

Dado que los delitos de ransomware suelen implicar a delincuentes, objetivos y víctimas, proveedores de servicios, instituciones financieras o sistemas informáticos en múltiples jurisdicciones, el uso eficaz de estas disposiciones en materia de cooperación internacional es especialmente importante.

El Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia (STCE 224)

El 12 de mayo de 2022 se abrió a la firma el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia (STCE 224). Una vez en vigor, este instrumento dotará a las Partes que lo integran de herramientas adicionales para favorecer la "cooperación reforzada y la divulgación de pruebas electrónicas". Dichas herramientas serán pertinentes, y en algunos casos muy pertinentes, para las investigaciones y procedimientos penales relacionados con los delitos de ransomware, e incluyen:

- Artículo 6 - Solicitud de información sobre el registro de nombres de dominio directamente a una entidad de otra Parte que preste servicios de registro de nombres de dominio;
- Artículo 7 - Divulgación de la información de los abonados mediante la cooperación directa con un proveedor de servicios de otra Parte;

- Artículo 8 - Dar efecto a las órdenes de otra Parte para la producción acelerada de información sobre los abonados y datos de tráfico;
- Artículo 9 - Divulgación acelerada de datos informáticos almacenados en caso de emergencia;
- Artículo 10 – Asistencia mutua en caso de emergencia;
- Artículo 11 – Videoconferencia;
- Artículo 12 – Equipos conjuntos de investigación e investigaciones conjuntas.

El ámbito de aplicación de este Protocolo vuelve a ser amplio en el sentido de que se aplicará no solo a los delitos relacionados con los sistemas y datos informáticos, sino también a la obtención de pruebas en forma electrónica de cualquier delito (véase el artículo 2.1.a).

Las condiciones y salvaguardias del artículo 13 aseguran que el establecimiento, ejecución y aplicación de las facultades y procedimientos previstos en el Protocolo estén sujetos a las condiciones y salvaguardias previstas en el derecho interno de cada una de las Partes, que debe garantizar la protección adecuada de los derechos humanos y las libertades. Además, en vista de que muchas Partes en el presente Protocolo, a fin de cumplir sus obligaciones constitucionales o internacionales, pueden verse obligadas a garantizar la protección de los datos personales, el artículo 14 establece salvaguardias de protección de datos que permiten a las Partes cumplir esas exigencias y asegura que los datos personales puedan transferirse cuando se haga uso de estas formas de cooperación rápida.

Declaración del T-CY

El T-CY está de acuerdo en que:

- los delitos relacionados con ataques de ransomware pueden comprender conductas que deben penalizarse de conformidad con los artículos 2 a 8, así como con el artículo 11 (tentativa y complicidad), y que pueden conllevar que se exija responsabilidad a las personas jurídicas en virtud del artículo 12 del Convenio sobre la Ciberdelincuencia;
- las medidas procesales y las herramientas de cooperación internacional del Convenio se podrán utilizar para investigar y perseguir los ataques de ransomware y los delitos conexos, así como su facilitación, participación en dichos delitos o actos preparatorios;

– el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, una vez en vigor, proporcionará a sus Partes herramientas adicionales para mejorar la cooperación y la divulgación de pruebas electrónicas relacionadas con los ataques de ransomware.

Nota de orientación sobre el Ámbito de aplicación de las facultades procesales y las disposiciones en materia de cooperación internacional del Convenio de Budapest

1. Introducción

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la Ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y aplicación efectivas del Convenio de Budapest sobre la Ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y tecnológicas.[73] Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

En la presente nota se aborda el alcance de las facultades procesales nacionales y de las disposiciones en materia de cooperación internacional del Convenio sobre la Ciberdelincuencia (STE 185), así como de su Segundo Protocolo Adicional relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas (STCE 224).

Si bien el texto del Convenio sobre la Ciberdelincuencia deja bastante claro que las facultades procesales y las disposiciones sobre cooperación internacional son aplicables no sólo a la ciberdelincuencia (artículos 2 a 11 del Convenio), sino también a "otros delitos cometidos mediante el uso de un sistema informático"; y a "la obtención de pruebas electrónicas de cualquier delito" (véase el artículo 14. 2. b y c y, de forma similar, los artículos 23 y 25 del STE 185), y aunque esto se confirma de nuevo en el Segundo Protocolo Adicional del Convenio (véase el artículo 2 del STCE 224), este ámbito de aplicación no siempre se comprende plenamente, y las legislaciones de algunos países limitan la aplicación de las facultades procesales o de las disposiciones en materia de cooperación internacional a un conjunto de ciberdelitos.

Por lo tanto, el T-CY decidió que una Nota de orientación, en la que se subraye cómo pueden aplicarse las disposiciones clave en materia de procedimiento y cooperación internacional no sólo a los delitos contra de sistemas informáticos y por medio de ellos, sino a una serie de delitos, sería beneficiosa desde el punto de vista práctico y estratégico.

73. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).

2. Disposiciones pertinentes del Convenio sobre la Ciberdelincuencia (STE 185)

2.1. Disposiciones sobre procedimiento

En virtud del Convenio sobre la Ciberdelincuencia "[c]ada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a" adoptar las medidas procesales previstas en los artículos 16 a 21 del Convenio:

- Artículo 16 – Conservación rápida de datos informáticos almacenados
- Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico
- Artículo 18 – Orden de presentación
- Artículo 19 – Registro y confiscación de datos informáticos almacenados
- Artículo 20 – Obtención en tiempo real de datos relativos al tráfico
- Artículo 21 – Interceptación de datos relativos al contenido

Estas medidas están sujetas a las condiciones y salvaguardias establecidas en el artículo 15.

El ámbito de aplicación de estas medidas procesales se define en el artículo 14:

> **Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento**
>
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos.
>
> 2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:
>
> a. los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
>
> b. otros delitos cometidos por medio de un sistema informático; y
>
> c. la obtención de pruebas electrónicas de cualquier delito.
>
> 3 a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de

limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y

ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.

Por lo tanto, según el artículo 14.2 del Convenio, las facultades procesales son aplicables a la obtención de pruebas en formato electrónico de cualquier delito. 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" del Convenio (párrafo 141 del Informe explicativo del Convenio).

En el párrafo 3 del artículo 14 se prevé excepciones a este amplio ámbito de aplicación y permite a las Partes restringir el ámbito de aplicación de las facultades más intrusivas (la obtención en tiempo real de datos relativos al tráfico en virtud del artículo 20 y la interceptación de datos relativos al contenido en virtud del artículo 21).[74]

Por lo tanto, las autoridades competentes pueden ordenar la conservación de datos, ordenar la presentación de datos, registrar o confiscar datos informáticos almacenados, u ordenar o llevar a cabo la obtención en tiempo real de datos relativos al tráfico o la interceptación de datos relativos al contenido[75] en investigaciones penales específicas relacionadas con cualquier delito tipificado en la legislación nacional, lo que incluye, por ejemplo:[76]

– corrupción;

74. Véanse las reservas y declaraciones de las Partes con respecto al artículo 14.
75. Como se indica en los artículos 20 y 21 del Convenio, pueden aplicarse restricciones a las facultades de obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido, como la limitación a una serie de delitos graves.
76. Véanse también las referencias que figuran a continuación a los tratados internacionales pertinentes que cubren algunos de estos delitos.

- falsificación de medicamentos u otras amenazas para la salud pública, incluidos los delitos relacionados con la COVID-19;
- diferentes formas de abuso de menores;
- diferentes formas de violencia familiar y contra las mujeres;
- diferentes formas de delitos económicos y financieros;
- delitos relacionados con las drogas;
- fraude;
- secuestro;
- manipulación de competiciones deportivas;
- blanqueo de dinero y financiación del terrorismo;
- asesinato;
- delitos relacionados con la delincuencia organizada;
- violación y otras formas de violencia sexual;
- terrorismo;
- genocidio, crímenes contra la humanidad, crímenes de guerra y otros crímenes internacionales;
- trata de seres humanos;
- xenofobia y racismo y otras formas delictivas de discursos de odio.

2.2. Disposiciones en materia de cooperación internacional

El amplio ámbito de aplicación de las facultades procesales nacionales se extiende a los principios y medidas relacionados con la cooperación internacional (capítulo III del Convenio). En los artículos 23 y 25 se deja claro que la cooperación no sólo es posible a efectos de investigaciones o procedimientos relativos a delitos relacionadas con sistemas y datos informáticos, sino también para la obtención de pruebas en formato electrónico de un delito:

> **Artículo 23 - Principios generales relativos a la cooperación internacional**
>
> Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, 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, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Artículo 25 –Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

En el párrafo 243 del Informe explicativo del Convenio se confirma que:

> "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."

Las Partes pueden restringir este amplio ámbito de aplicación en lo que respecta a la asistencia mutua para la obtención en tiempo real de datos relativos al tráfico (artículo 33) y a la asistencia mutua en relación con la interceptación de datos relativos al contenido (artículo 34). Además, la cooperación internacional puede estar sujeta a condiciones, como requisitos de doble tipificación penal,[77] o motivos de denegación en consonancia con los artículos 25.4, 27.4 y 27.5[78] del Convenio.

Los principios y las medidas para la cooperación internacional sobre los delitos enumerados en el Convenio y otros delitos cometidos por medio de un sistema informático, así como la obtención de pruebas electrónicas de cualquier otro delito, están previstos en los artículos 23 a 35[79] del Convenio:

- Artículo 23 – Principios generales relativos a la cooperación internacional;
- Artículo 25 – Principios generales relativos a la asistencia mutua;
- Artículo 26 – Información espontánea;

77. Véase el artículo 29.4 del Convenio. Como se señala en el párrafo 259 del Informe explicativo del Convenio, "...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."
78. El artículo 27.5 del Convenio se refiere a los motivos para posponer una actuación en respuesta a una solicitud.
79. Nota: La obligación de otorgar la extradición en virtud del "Artículo 24 - Extradición" se aplica solo "a los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave."

- Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables;
- Artículo 28 – Confidencialidad y restricciones de uso;
- Artículo 29 – Conservación rápida de datos informáticos almacenados;
- Artículo 30 – Revelación rápida de datos conservados;
- Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados;
- Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público;
- Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico;
- Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido;
- Artículo 35 – Red 24/7.

Las Partes en el Convenio podrán hacer uso de estas medidas y principios para cooperar entre sí en la mayor medida posible a efectos de investigaciones o procedimientos penales y de obtención de pruebas en forma electrónica de cualquier delito, y solicitar la conservación de datos, el acceso a datos informáticos almacenados, la obtención en tiempo real de datos relativos al tráfico o la interceptación de datos relativos al contenido[80], o acceder a datos informáticos almacenados transfronterizos con consentimiento o cuando sean accesibles al público, en relación con cualquier delito y en las condiciones estipuladas en el capítulo III del Convenio.

3. Disposiciones pertinentes del Segundo Protocolo Adicional (STCE 224)

El 12 de mayo de 2022 se abrió a la firma el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia (STCE 224). Una vez en vigor, este

80. Como se indica en los artículos 20 y 21 del Convenio, pueden aplicarse restricciones a las facultades de obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido, como la limitación a una serie de delitos graves. En cuanto a los artículos 33 y 34 correspondientes sobre cooperación internacional, "Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno" (artículo 33.2), y en cuanto a la interceptación de datos relativos al contenido "Las Partes se prestarán asistencia mutua... en la medida en que lo permitan sus tratados y leyes internas aplicables" (artículo 34).

instrumento dotará a las Partes que lo integran de herramientas adicionales para favorecer la "cooperación reforzada y la divulgación de pruebas electrónicas".

El ámbito de aplicación de este Protocolo vuelve a ser amplio en el sentido de que se aplicará no solo a los delitos relacionados con los sistemas y datos informáticos, sino también a la obtención de pruebas en forma electrónica de cualquier delito:

> **Artículo 2 – Ámbito de aplicación**
>
> 1. Salvo que se especifique lo contrario en el presente Protocolo, las medidas descritas en el presente Protocolo se aplicarán:
>
>   a. entre las Partes en el Convenio que sean Partes en el presente Protocolo, a las investigaciones o procedimientos penales específicos relativos a los delitos relacionados con sistemas y datos informáticos, y a la obtención de pruebas en forma electrónica de un delito penal; y
>
>   b. en lo que respecta a las Partes en el Primer Protocolo que sean Partes en el presente Protocolo, a investigaciones o procedimientos penales específicos relativos a delitos penales tipificados con arreglo al Primer Protocolo.

Las medidas previstas en el presente protocolo son:

- Artículo 6 – Solicitud de información sobre el registro de nombres de dominio directamente a una entidad de otra Parte que preste servicios de registro de nombres de dominio;
- Artículo 7 – Divulgación de la información de los abonados mediante la cooperación directa con un proveedor de servicios de otra Parte;
- Artículo 8 – Dar efecto a las órdenes de otra Parte para la producción acelerada de información sobre los abonados y datos de tráfico;
- Artículo 9 – Divulgación acelerada de datos informáticos almacenados en caso de emergencia;
- Artículo 10 – Asistencia mutua en caso de emergencia;
- Artículo 11 – Videoconferencia;
- Artículo 12 – Equipos conjuntos de investigación e investigaciones conjuntas.

Estas medidas están sujetas a las condiciones y salvaguardias de los artículos 13 y 14 del STCE 224.

Por lo tanto, las autoridades competentes de las Partes en el presente Protocolo podrán - sin perjuicio de las reservas y declaraciones que se permitan de

conformidad con el artículo 19 del STCE 224 - solicitar información sobre el registro de nombres de dominio, ordenar la divulgación de la información de los abonados, dar curso a órdenes de presentación de información sobre información de los abonados y datos relativos al tráfico, cooperar en casos de emergencia, hacer uso de videoconferencias o establecer equipos conjuntos de investigación o participar en investigaciones conjuntas relacionadas con investigaciones o procedimientos penales relativos a delitos relacionados con sistemas y datos informáticos, y con la obtención de pruebas en formato electrónico de cualquier delito.

4. Sinergias entre el Convenio sobre la ciberdelincuencia y otros tratados

Las facultades procesales nacionales y los principios y medidas de cooperación internacional también se podrán utilizar para obtener pruebas electrónicas relacionadas con delitos previstos en otros acuerdos internacionales en los que los Estados sean Partes, con sujeción a las condiciones pertinentes señaladas anteriormente.[81] Dichos acuerdos pueden incluir los relativos a la corrupción;[82] la falsificación de medicamentos u otras amenazas para la salud pública[83]; el abuso de menores[84]; la violencia doméstica y la violencia contra las mujeres[85]; los delitos relacionados con las drogas;[86] la manipulación de competiciones deportivas[87]; el blanqueo de dinero y la financiación del terrorismo[88]; los delitos

81. Como los requisitos de doble tipificación penal, o los motivos de denegación en consonancia con los artículos 25.4 y 27.4 del Convenio
82. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio de Derecho penal contra la corrupción (STE núm. 173) del Consejo de Europa o la Convención de las Naciones Unidas contra la Corrupción.
83. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio del Consejo de Europa sobre la falsificación de productos médicos y delitos similares que supongan una amenaza para la salud pública (STCE núm. 211)
84. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y los abusos sexuales (STCE núm. 201)
85. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica (STCE núm. 210)
86. Por ejemplo, las conductas delictivas a las que se hace referencia en los tratados de fiscalización de drogas de las Naciones Unidas
87. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio del Consejo de Europa sobre Manipulación de Competiciones Deportivas (STCE núm. 215)
88. Por ejemplo, las conductas delictivas a las que hace referencia en el Convenio del Consejo de Europa relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito y a la financiación del terrorismo (STCE núm. 198)

relacionados con la delincuencia organizada;[89] el terrorismo;[90] la trata de seres humanos;[91] o el genocidio, los crímenes contra la humanidad, los crímenes de guerra y otros crímenes internacionales.[92]

Para las Partes del primer Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE 189),[93] el artículo 8.2 estipula que las "Partes harán extensivo el ámbito de aplicación de las medidas definidas en los artículos 14 a 21 y en los artículos 23 a 35 del Convenio a los artículos 2 a 7 del presente Protocolo".

En 2018, el T-CY recomendó que se alentara a las Partes del Convenio de Lanzarote para la protección de los niños contra la explotación y el abuso sexual (STCE 201) y del Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica (STCE 210) "a introducir las facultades procesales de los artículos 16 a 21 del Convenio de Budapest en la legislación nacional y a considerar la posibilidad de convertirse en Partes del Convenio de Budapest para facilitar la cooperación internacional en materia de pruebas electrónicas (artículos 23 a 35 del Convenio de Budapest) en relación con la violencia sexual en línea contra los niños y la violencia contra las mujeres y la violencia familiar".[94]

5. Declaración del T-CY

El T-CY está de acuerdo en que las disposiciones de derecho procesal y los principios y medidas para la cooperación internacional del Convenio sobre la ciberdelincuencia son aplicables no sólo a los delitos relacionados con los

89. Por ejemplo, las conductas delictivas a las que se hace referencia en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos.
90. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio del Consejo de Europa para la Prevención del Terrorismo (STCE núm. 196) y sus Protocolos.
91. Por ejemplo, las conductas delictivas a las que se hace referencia en el Convenio del Consejo de Europa sobre la Lucha contra la Trata de Seres Humanos (STCE núm. 197)
92. Por ejemplo, las conductas delictivas a las que se hace referencia en la Convención para la Prevención y la Sanción del Delito de Genocidio de 1948, los cuatro Convenios de Ginebra sobre Derecho Internacional Humanitario y sus Protocolos Adicionales de 1949 o el Estatuto de Roma de la Corte Penal Internacional.
93. Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE núm. 189)
94. Véase el Estudio cartográfico del T-CY sobre la ciberviolencia https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

sistemas y datos informáticos, sino también a la obtención de pruebas electrónicas de cualquier delito. Este amplio ámbito de aplicación también se aplica a las medidas del Segundo Protocolo Adicional al Convenio.

Este ámbito de aplicación permite además establecer sinergias entre el Convenio de Budapest y otros acuerdos internacionales.

PREMS 105123

SPA

www.coe.int

El Consejo de Europa es la principal organización del continente que defiende los derechos humanos. Cuenta con 46 Estados miembros, incluidos todos los miembros de la Unión Europea. Todos los Estados miembros han suscrito el Convenio Europeo de Derechos Humanos, tratado concebido para proteger los derechos humanos, la democracia y el Estado de derecho. El Tribunal Europeo de Derechos Humanos supervisa la aplicación del Convenio en los Estados miembros.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE