Proyecto sobre cibercriminalidad
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Versión [10 March 2010]

Legislación sobre cibercriminalidad

PORTUGAL

Este perfil se ha preparado en el marco de la capacidad del Consejo de Europa sobre el delito cibernético de compartir información y evaluar el estado actual de la aplicación de la Convención sobre el delito cibernético en virtud de la legislación nacional de proyectos de construcción. No refleja necesariamente posiciones oficiales del país cubierto o del Consejo de Europa.

Comentarios deberán ser mandados a:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

País	**Portugal**
Firma de la Convención:	**Si, el 23 de Noviembre del 2001**
Ratificación:	**Si, el 24 de Marzo del 2010**
Disposiciones de la Convención	
Capitulo 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;	**Ley nº 109/2009 (15 de septiembre)** **Artículo 2 - Definiciones** Para los efectos de la presente ley, se considera: a) «sistema informático», cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de datos informáticos, así como la red que soporta ésta comunicación entre ellos y el conjunto de datos informáticos

b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función; 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; d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.	almacenados, tratados, recuperados o transmitidos por aquel o aquellos dispositivos con vistas a su funcionamiento, utilización, protección y mantenimiento; b) «datos informáticos», toda representación de hechos, informaciones o conceptos de una forma adecuada para su procesamiento en un sistema informático, incluidos los programas capaces de hacer que un sistema informático ejecute una función; c) «datos de tráfico», los datos informáticos relativos a una comunicación efectuada por medio de un sistema informático, generados por este sistema como elemento de una cadena de comunicación, indicando el origen de la comunicación, su destino, su trayecto, la hora, la fecha, el tamaño, duración o el tipo de servicio subyacente; d) «proveedor de servicios»: cualquier entidad, pública o privada, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema informático, así como cualquier otra entidad que procesa o almacena datos informáticos en nombre y por cuenta de aquella entidad proveedora o de sus usuarios; e) «intercepción»: el acto destinado a captar la información contenida en un sistema informático, utilizando dispositivos electromagnéticos, acústicos, mecánicos u otros; f) «topografía», una serie de imágenes unidas entre sí, independientemente de como estén fijadas o codificadas, que representan la configuración tridimensional de las capas de un producto semiconductor y en el cual cada imagen reproduce el dibujo, o parte de ello, de una superficie del producto semiconductor, en cualquier etapa de su fabricación; g) «producto semiconductor», la forma final o intermedia de cualquier producto, que comprende un sustrato que incluye una capa de material semiconductor y constituido por una o más capas de materiales conductores, aislantes o semiconductores, según una disposición conforme a una configuración en tres dimensiones y destinada a desempeñar, exclusivamente o no, una función electrónica.
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 resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 6 - Acceso ilegítimo** 1. Quien, sin permiso legal o sin estar autorizado por el propietario, por otro titular del derecho del sistema o de una parte del mismo, acceda de cualquier modo a un sistema informático, será penado con pena de prisión de hasta 1 años o con pena de multa de hasta 120 días. 2. En la misma pena incurrirá quien ilegítimamente produzca, venda, distribuya, o de cualquier otra forma disemine o introduzca en uno o mas sistemas informáticos, dispositivos, programas, un conjunto ejecutable de instrucciones, un código u otros datos informáticos destinados a producir las acciones no autorizadas descritas en el número anterior. 3. Se impondrá pena de prisión de hasta 3 años o multa, al acceso logrado por medio de la violación de las reglas de seguridad. 4. La pena de prisión de 1 a 5 años se impondrá cuando: a. a través del acceso, el agente haya tomado conocimiento de un secreto comercial o industrial o de datos confidenciales, protegidos por la ley, o, b. el beneficio o ventaja patrimonial obtenidos fueran de un valor considerablemente elevado. 5. La tentativa es punible, salvo en los casos previstos en el número 2. 6. En los casos previstos en los números 1, 3 y 5 el procedimiento depende de denuncia privada.
Artículo 3 – Interceptación ilícita Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.	**Ley nº 109/2009 (15 de septiembre)** **Interceptación ilegítima** 1. Quien, sin permiso legal o sin estar autorizado por el propietario, por el titular de otro derecho sobre el sistema o parte del mismo, a través de medios técnicos, intercepte transmisiones de datos informáticos que se procesan en el interior de un sistema informático, a él destinadas o provenientes de él, será penado con pena de hasta 3 años o pena de multa. 2. La tentativa es punible. 3. incurre en la misma pena prevista en el nro. 1 quien ilegítimamente produzca, venda, distribuya o por cualquier otra forma disemine o introduzca en uno o más sistemas informáticos, dispositivos, programas u otros datos informáticos destinados a producir las acciones no autorizadas descritas en el mismo número.

Artículo 4 – Ataques a la integridad de los datos 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.	**Ley nº 109/2009 (15 de septiembre)** 1. Quien, sin permiso legal o sin estar autorizado por el propietario, por otro titular de derechos del sistema o de parte del mismo, anule, altere, destruya en todo o en parte, cancele, suprima o torne inutilizables o no accesibles programas u otros datos informáticos ajenos o que de cualquier otra forma afecte su capacidad de uso, será penado con pena de prisión hasta 3 años o pena de multa. 2. La tentativa es punible. 3. Incurre en la misma pena del nro. 1 quien ilegítimamente produzca, venda, distribuya o, de cualquier otra forma disemine o introduzca en uno o más dispositivos o sistemas informáticos destinados a producir las acciones no autorizadas descritas en ese número. 4. Si el daño causado fuera de valor elevado, la pena de prisión será hasta 5 años o de multa hasta 600 días. 5. Si el daño causado fuera de valor considerablemente elevado, la pena será de prisión de 1 a 10 años. 6. En los casos previstos en los artículos 1,2 y 4 el procedimiento penal dependerá de denuncia privada.
Artículo 5 – Ataques a la integridad del sistema Cada Parte adoptará las medidas legislativas y de otro tipo que resulten 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, daño, borrado, deterioro, alteración o supresión de datos informáticos.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 5 - Sabotaje informático** 1. Quien, sin permiso legal o sin estar autorizado por el propietario, por otro titular del derecho del sistema o departe del mismo, entorpezca, impida, interrumpa o perturbe gravemente el funcionamiento de un sistema informático, a través de la introducción, transmisión, deterioro, daño, alteración, cancelación, impedimento de acceso o supresión de programas u otros datos informáticos, o cualquier otra forma de interferencia en un sistema informático, será penado con pena de prisión hasta 5 años o con pena de multa de hasta 600 días. 2. En la misma pena incurrirá quien ilegítimamente produzca, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos, programas u otros datos informáticos destinados a producir las acciones no autorizadas descritas en el número anterior. 3. En los casos previstos en el número anterior, la tentativa no es punible. 4. La pena será de de 1 a 5 años de prisión si el daño provocado por la perturbación es de un valor elevado. 5. Se impondrá pena de prisión de 1 a 10 años: a. Al daño emergente de la perturbación por el valor considerablemente elevado, b. a la perturbación de forma grave o duradera a un sistema informático que

	fomente una actividad destinada a asegurar funciones sociales críticas, sobretodo cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los servicios públicos.
Artículo 6 – Abuso de los dispositivos 1. 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 los siguientes actos: a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i. cualquier 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; ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención 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 incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. 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. 2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático. 3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas	**Ley nº 109/2009 (15 de septiembre)** **Artículo 3 - Falsificación informática** 4. Quien importe, distribuya, venda o tenga con fines comerciales cualquier dispositivo que permita el acceso a un sistema o medio de pago, a un sistema de comunicaciones o a un servicio de acceso condicionado, sobre el cual realice las acciones previstas en el nro. 2 será penado con pena de prisión de 1 a 5 años. **Artículo 4 - Daño relativo a programas o otros datos informáticos** 3. Incurre en la misma pena del nro. 1 quien ilegítimamente produzca, venda, distribuya o, de cualquier otra forma disemine o introduzca en uno o más dispositivos o sistemas informáticos destinados a producir las acciones no autorizadas descritas en ese número **Artículo 5 - Sabotaje informático** 2. En la misma pena incurrirá quien ilegítimamente produzca, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos, programas u otros datos informáticos destinados a producir las acciones no autorizadas descritas en el número anterior. **Artículo 6 - Acceso ilegítimo** 2. En la misma pena incurrirá quien ilegítimamente produzca, venda, distribuya, o de cualquier otra forma disemine o introduzca en uno o mas sistemas informáticos, dispositivos, programas, un conjunto ejecutable de instrucciones, un código u otros datos informáticos destinados a producir las acciones no autorizadas descritas en el número anterior. **Artículo 7 - Interceptación ilegítima** 3. incurre en la misma pena prevista en el nro. 1 quien ilegítimamente produzca, venda, distribuya o por cualquier otra forma disemine o introduzca en uno o más sistemas informáticos, dispositivos, programas u otros datos informáticos destinados a producir las acciones no autorizadas descritas en el mismo número.

Título 2 – Delitos informáticos	
Artículo 7 – Falsificación informática Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 3 - Falsificación informática** 1. Quien con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir datos informáticos, o interferir de cualquier otra forma en el tratamiento informático de datos, produciendo datos o documentos no genuinos, con intención de que estos fueran considerados o utilizados para finalidades jurídicamente relevantes, será penado con prisión de hasta 5 años y multa de 120 a 600 días. 2. Cuando las acciones descritas en el número anterior incidieran sobre los datos registrados o incorporados en una carta bancaria de pago o en cualquier otro dispositivo que permita el acceso a un sistema o medio de pago, a un sistema de comunicaciones o a un servicio de acceso condicionado, será penado con penas de 1 a 5 años de prisión. 3. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento producido a partir de datos informáticos que fueran objeto de los actos referidos en el nro. 1, o carta u otro dispositivo en el cual se encuentren registrados o incorporados los datos objeto de las conductas referidas en el número anterior, será penado con las penas previstas en el número correspondiente. 4. Quien importe, distribuya, venda o tenga con fines comerciales cualquier dispositivo que permita el acceso a un sistema o medio de pago, a un sistema de comunicaciones o a un servicio de acceso condicionado, sobre el cual realice las acciones previstas en el nro. 2 será penado con pena de prisión de 1 a 5 años. 5. Si los hechos referidos en los números anteriores fueren realizados por un funcionario en el ejercicio de sus funciones, la pena será de 2 a 5 años de prisión.
Artículo 8 – Fraude informático Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático,	**CÓDIGO PENAL** **Artículo 221 - Fraude informático y en las comunicaciones** 1 - Toda persona que, con la intención de obtener para sí o para tercero enriquecimiento ilegítimo, causando pérdidas económicas a otra persona, interfiriendo con el resultado de tratamiento de datos o mediante una incorrecta estructuración de software, uso incorrecto o incompletos de datos, uso no autorizado de datos o por intervención de cualquier otra manera no autorizada en el procesamiento, será punido con prisión de hasta 3 años o multa.

con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.	2 - La misma pena se aplica a aquellos que, con la intención de obtener para sí o para tercero un beneficio ilegítimo, causen pérdida económica a tercero, utilizando software, dispositivos electrónicos u otros medios que, por separado o en conjunto, tienen por objeto disminuir, alterar o impedir, en todo o en parte el funcionamiento normal o la explotación de servicios de telecomunicaciones. 3 – El intento es punible. 4 – El procedimiento depende de denuncia. 5 - Si el prejuicio es: a) de valor elevado, el agente es punido con pena de prisión de hasta 5 años o multa de hasta 600 días; b) de valor considerablemente elevado, el agente es punido con pena de prisión de 2 a 8 años. 6 – Se aplican, correspondientemente las disposiciones del artículo 206.
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 resulten 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 la intención de difundirla a través de un sistema informático; b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático; c. la difusión o la transmisión de pornografía infantil a través de un sistema informático; d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos. 2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de: a. un menor adoptando un comportamiento sexualmente explícito; b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito; c. imágenes realistas que representen a un menor adoptando un	**CÓDIGO PENAL** **Artículo 176 - Pornografía de menores** 1 - Quién: a) Utilice menor en espectáculo pornográficos o lo tentar con este fin; b) Utilice menor en fotografía, película o grabación pornográficas, cualquiera que sea su soporte, o lo tentar con este fin; c) Producir, distribuir, importar, exportar, promocionar, exhibir o vender, en cualquier forma o por cualquier medio, los materiales descritos en el párrafo anterior; d) Adquirir o detuviere materiales descritos en la letra b) con la intención de distribuir, importar, exportar, promocionar, exhibir o vender; es punido con prisión de uno a cinco años. 2 - Quien practique los actos descritos en el apartado anterior profesionalmente o con fines de lucro, será castigado con prisión de uno a ocho años. 3 - Quien practique los actos descritos en las letras c) y d) del apartado 1, utilizando material pornográfico con representación realista de menores es punido con pena de prisión de hasta dos años. 4 - Quién adquirir o detuviere los materiales descritos en la letra b) del apartado 1, será punido con prisión de hasta un año o multa. 5 – El intento es punible.

comportamiento sexualmente explícito. 3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años. 4. Las Partes podrán reservarse el derecho a no aplicar, en todo 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 resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual 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 Derecho de Autor, 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 legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que 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 conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 8 - Reproducción ilegítima de programa protegido** 1. Quien, ilegítimamente reproduzca, divulgue o comunique al público un programa informático protegido por ley será penado con pena de prisión de hasta 3 años o con pena de multa. 2. En la misma pena incurrirá quien ilegítimamente reproduzca topografía de un producto semiconductor o la explorar comercialmente o importar, a tales fines, una topografía o un producto semiconductor fabricado a partir de esa topografía. 3. La tentativa es punible. **Decreto-Ley No. 252/94 del 20 de octubre** **Artículo 14 - Tutela Penal** 1 - Un programa de ordenador está penalmente protegido contra la reproducción no autorizada. 2 - Se aplican al programa de ordenador las disposiciones del apartado 1 del artículo 9 de la Ley No. 109/91 del 17 de agosto. (*esta ley fue derogada y sustituida por la Ley N º 109/2009, y el artículo 9, apartado 1 se sustituye por el nuevo artículo 8, apartado 1*) **Ley N º 45/85, 17 de septiembre, alterada por la Ley N º 16/2008 (Código de Derecho de Autor)** **Artículo 195 - Usurpación** 1 - Comete el delito de usurpación quién, sin autorización del autor o artista, productor de fonogramas y videogramas o del organismo de radiodifusión, utilizar una obra o prestación por cualquiera de las formas previstas en este Código.

3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer 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.	2 - También comete el delito de usurpación: a) El que ilegítimamente difunda o publique una obra no divulgada ni publicada por su autor o no destinada a la difusión o publicación, incluso si se presenta como siendo de su respectivo autor, sea o no obtiene animado por intuito de obtener ventaja económica; b) Quién recopila o reúne obras inéditas o publicadas sin permiso del autor; c) Quién, estando autorizado a utilizar una obra, prestación de artista, fonograma, videogramas o emisión radiodifundida exceder los limites de autorización, salvo en los casos previstos expresamente en el presente Código. 3 - Será punido con las penas previstas en el artículo 197 el autor, habiendo transmitido, en su totalidad o en parte, sus derechos o habiendo autorizado el uso de su obra por cualquier forma prevista en este Código, la utilizar directa o indirectamente con ofensa a los derechos asignados a otras personas. **Artículo 196 - Falsificación** 1 - Comete el delito de falsificación quién utilizar, como si fuera su creación o prestación, el trabajo, prestación de artista, fonograma, videogramas, la emisión de radiodifusión que es total o parcial mera reproducción de obra o prestación de tercero, divulgada o no divulgada, o tan similar que no tiene individualidad. 2 - Si la reproducción mencionada en el apartado anteriormente representa solamente una parte o fracción de la obra o prestación, sólo esa parte o fragmento es considerado falsificación. 3 - Para que exista falsificación no es esencial que la reproducción sea hecha por el mismo procedimiento que el original, con las mismas dimensiones o con el mismo formato. 4 - No constituye falsificación: a) La semejanza entre traducciones debidamente autorizados de la misma obra, o entre fotografías, grabados, dibujos, u otras formas de representación del mismo objeto, si, a pesar de las similitudes, debido a la identidad del objeto, cada una de las obras tiene su individualidad propia; b) la reproducción por la fotografía o grabado efectuada sólo con el propósito de la documentación de la crítica artística. **Articulo 199 - Aprovechamiento de obra falsificada o usurpada** 1 – Quién venda, ofrezca en venta, importe, exporte o distribuya al publico obra usurpada o falsificada o copia no autorizada de fonograma o videograma, si las copias se han producido en el país o en el extranjero, será punido con las penas

	descritas en artículo 197. 2 - La negligencia es punible con multa de hasta 50 días. **Artículo 218 - Tutela Penal** 1 – Quién, no estando autorizado, neutralizar cualquier medida eficaz de carácter tecnológico, sabiéndolo o teniendo motivos razonables para saberlo, será punido con prisión de hasta 1 año o multa de hasta 100 días. 2 - El intento es punido con multa de hasta 25 días. **Artículo 224 - Tutela Penal** 1 - Quién, no estando autorizado, intencionalmente, sabiéndolo o teniendo motivos razonables para saberlo, practique uno de los siguientes actos: a) suprima o cambie cualquier información para la gestión electrónica de derechos; b) distribuya, importación para distribución, comunique por radiodifusión, o ponga a disposición del público obras, interpretaciones o producciones protegidas, de las cuales ha sido suprimida o alterada sin autorización la información para la gestión electrónica de derechos, sabiendo que en cualquier de las situaciones enumeradas se provoca, permite, facilita o encubre una violación de los derechos de propiedad intelectual; es punido con penas de prisión de hasta 1 año o multa de hasta 100 días. 2 - El intento es punido con multa de hasta 25 días.
Título 5 – Otras formas de responsabilidad y de sanción	
Artículo 11 – Tentativa y complicidad 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio. 3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.	**CÓDIGO PENAL** **Artículo 22 - Intento** 1 – Hay intento cuando el agente practica actos de ejecución de un delito que ha decidido cometer, sin que este se llegue a consumar. 2 - Son actos de ejecución: a) Los que constituyan elemento de un tipo de delito; b) Los que son idóneos a producir el resultado típico, o c) Los que, según la experiencia común, y salvo circunstancias no previstas, son tales como para esperar que se le sigan los actos de las especies citadas en los párrafos anteriores. **Artículo 23 - Punición del intento**

	1 - A menos que se disponga en contrario, el intento es punible apenas si al respectivo delito consumado corresponda pena superior a tres años de prisión. 2 - El intento se pune con la pena aplicable al delito consumado, especialmente atenuada. 3 - El intento no es punible cuando es evidente la torpeza de los medios empleados por el agente o la falta del objeto esencial de la consumación del delito. **Artículo 27 - Complicidad** 1 - Es punible como cómplice quién, de forma deliberada y por cualquier forma prestar auxilio material o moral a la práctica por tercero de un hecho intencional. 2 - Se aplica al cómplice la pena fijada para el autor, especialmente atenuada.
Artículo 12 – Responsabilidad de las personas jurídicas 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de: a. un poder de representación de la persona jurídica; b. una autorización para tomar decisiones en nombre de la persona jurídica; c. una autorización para ejercer funciones de control en el seno de la persona jurídica. 2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad. 3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 9 - Responsabilidad penal de las personas jurídicas y entidades similares** Las personas jurídicas y entidades equiparadas son penalmente responsables por los crímenes previstos en la presente ley en los términos y límites del régimen de responsabilidad previsto en el Código Penal.

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 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad. 2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.	No fue regulado en ninguna legislación específica, pero resulta de otras normas.
Sección 2 – Derecho procesal	
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. 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. 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	**Ley nº 109/2009 (15 de septiembre)** **Artículo 11 - Ámbito de aplicación de las disposiciones procesales** 1. Con excepción de lo dispuesto en los artículos 18º y 19º, las disposiciones procesales previstas en el presente capítulo se aplicarán a los procesos relativos a los delitos: a) previstos en la presente ley, b) cometidos por medio de un sistema informático; o c) en relación a los cuales sea necesario proceder a la recolección de prueba en soporte electrónico. 2. Las disposiciones procesales previstas en el presente capítulo no afectarán el régimen de la ley nº 32/2008, del 17 de julio.

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 de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.	
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.	No fue regulado en ninguna legislación específica, pero resulta de otras normas.

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.	
Artículo 16 – Conservación rápida de datos informáticos almacenados 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. 2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno. 4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 12 - Preservación expedita de los datos** 1. Si en el transcurso de un proceso fuera necesario a la producción de prueba, teniendo en vista el descubrimiento de la verdad, la obtención de datos informáticos específicos almacenados en un sistema informático, incluyendo datos de tráfico, en relación a los cuales haya temor de que puedan perderse, alterarse, o dejar de estar disponibles, la autoridad judicial competente ordenará a quien tenga la disponibilidad o el control de tales datos, incluido el proveedor de servicios que preserve los datos en cuestión. 2. La preservación puede ser también ordenada por la policía criminal mediante autorización de la autoridad judicial competente o cuando haya urgencia o peligro en la demora, debiendo aquél, en este último caso, dar noticia inmediata del hecho a la autoridad judicial y transmitirle el informe previsto en el artículo 253º del Código Procesal Penal. 3. La orden de preservación deberá distinguir, so pena de nulidad: a. la naturaleza de los datos, b. su origen y destino, si fueran conocidos; y c. el período de tiempo en el cual deberán ser preservados, hasta un máximo de 3 meses. 4. En cumplimiento de la orden de preservación que le fue dirigida, quien tenga la disponibilidad o control sobre esos datos, incluido el proveedor de servicios, deberá preservar de inmediato los datos en cuestión, protegiendo y conservando su integridad por el tiempo fijado, para permitir a la autoridad judicial competente su obtención, y está obligado a asegurar la confidencialidad de la aplicación de la medida procesal. 5. La autoridad judicial competente podrá ordenar la renovación de la medida por períodos sujetos al límite previsto en el punto "c" del nº 3, cuando se verifiquen los respectivos requisitos de admisibilidad, hasta el límite máximo de un año.
Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico	**Ley nº 109/2009 (15 de septiembre)** **Artículo 13 - Revelación expedita de los datos de tráfico**

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para: a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido. 2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	Con el fin de asegurar la preservación de los datos de tráfico relativos a una determinada comunicación, independientemente del número de proveedores de servicio que participaran de ella, el proveedor de servicio a quien esa preservación haya sido ordenada en los términos del artículo anterior informará a la autoridad judicial o a la policía criminal, ni bien lo sepa, otros proveedores de servicio por medio de los cuales aquella comunicación haya sido efectuada, con el fin de identificar a todos los proveedores de servicio a través de los cuales la comunicación ha sido efectuada.
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; 2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15. 3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de 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;	**Ley nº 109/2009 (15 de septiembre)** **Artículo 14 - Orden de presentación o acceso a datos** Si en el transcurso de un proceso fuera necesario para la obtención de prueba con el fin de descubrir la verdad, obtener datos informáticos específicos, almacenados en un sistema informático determinado, la autoridad judicial competente ordenará a quien tenga la disponibilidad o el control de tales datos que los comunique al proceso o que permita el acceso a los mismos, so pena de incurrir en el delito de desobediencia. La orden mencionada en el párrafo anterior identificará los datos en cuestión. 3. En cumplimiento de la orden descrita en los números 1 y 2, quien tenga disponibilidad o control de tales datos comunicará esos datos a la autoridad judicial competente o permitirá, so pena de responsabilidad por desobediencia, el acceso al sistema informático donde los mismos se encuentran almacenados. 4. Lo dispuesto en el presente artículo será aplicable a los proveedores de servicio, a quienes se les podrá ordenar que comuniquen los datos relativos a sus clientes o abonados, en los cuales se incluye toda información diferente de los datos de tráfico o de contenido que conste bajo el formato de datos informáticos o cualquier otra forma, contenida por el proveedor de servicios y que permita determinar: a. el tipo de servicio de comunicación utilizado, como las medidas técnicas

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.	tomadas a ese respecto o período de servicio; b. La identidad, el domicilio postal o geográfico y el número de teléfono del abonado, y cualquier otro número de acceso, los datos respectivos a la facturación o al pago, disponibles en base al contrato o acuerdo de servicios; o c. Cualquier otra información o acuerdo de servicios, o equipamiento de comunicación, disponible con base en un contrato o acuerdo de servicios. 5. La orden en virtud del presente artículo no podrá ser dirigida a un sospechoso o imputado en el proceso. 6. Tampoco se podrá hacer uso de la orden prevista en este artículo cuando los sistemas informáticos son utilizados para el ejercicio de la abogacía, de las actividades médicas y bancarias, o de la profesión de periodista. 7- El régimen de secreto profesional o de funcionario y de secreto de Estado previsto en el artículo 182º del Código Procesal Penal es aplicable con las adaptaciones necesarias.
Artículo 19 – Registro y confiscación de datos informáticos almacenados 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar: a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten	**Ley nº 109/2009 (15 de septiembre)** **Artículo 15 - Búsqueda de datos informáticos** 1. Cuando en el transcurso de un proceso fuera necesario con el fin de descubrir la verdad, obtener datos informáticos específicos y determinados, amenazados en un determinado sistema informático, la autoridad judicial competente autorizará u ordenará por orden que se proceda a un registro en el sistema informático, debiendo, en la medida de lo posible, presidir la diligencia. 2. La orden prevista en el número anterior tendrá un plazo de validez máximo de 30 días, so pena de nulidad. 3. La policía criminal podrá proceder a la pesquisa, sin previa autorización de la autoridad judicial, cuando: a. La misma fuera voluntariamente consentida por quien tuviera la disponibilidad o control de tales datos, cuando el consentimiento prestado se encuentre, por cualquier medio, documentado. b. en los casos de terrorismo, criminalidad violenta o altamente organizada, cuando haya indicios fundados de la comisión inminente de un delito que ponga en riesgo grave la vida o la integridad de cualquier persona. 4. Cuando la policía criminal proceda a la pesquisa en los términos del número anterior: a. en el caso previsto en el punto b), la realización de la diligencia será, bajo pena de nulidad, inmediatamente comunicada a la autoridad judicial competente y será apreciada por esta en orden a su validación.

necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas: a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático; b. realizar y conservar una copia de esos datos informáticos; c. preservar la integridad de los datos informáticos almacenados pertinentes; y d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado. 4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2. 5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	b) en cualquier caso, será elaborado y remitido a la autoridad judicial competente el informe previsto en el artículo 253º del Código Procesal Penal. 5. Cuando, en el transcurso de la investigación, surgieran razones para creer que los datos procurados se encuentran en otro sistema informático, o en una parte diferente del sistema registrado, si tales datos son legítimamente accesibles a partir del sistema inicial, el registro podrá ser extendido mediante autorización u orden de autoridad competente en los términos de los números 1 y 2. 6. En los registros a los que se refiere este artículo serán aplicables, con las necesarias adaptaciones, las reglas de ejecución de búsquedas previstas en el Código Procesal Penal y en el Estatuto del Periodista. **Artículo 16 - Secuestro de datos informáticos** 1 - Cuando, en una búsqueda u otro acceso legítimo a un sistema informático, se encontraran datos o documentos informáticos necesarios para la producción de pruebas, a fin de establecer la verdad, la autoridad judicial autorizará u ordenará por orden la incautación de los mismos. 2 - La policía criminal podrá incautar, sin previa autorización judicial, en el curso de un registro legítimamente ordenado y realizado de conformidad con el artículo anterior, y también podrá hacerlo en casos de emergencia o cuando haya peligro de demora. 3 – Cuando se incauten datos o documentos informáticos cuyo contenido sea susceptible de revelar datos personales o íntimos, que puedan poner en peligro la privacidad de su propietario o de tercero, bajo pena de nulidad, tales datos o documentos se presentarán ante el juez, quien decidirá de su incautación, teniendo en cuenta los intereses del caso concreto. 4 - La incautación efectuada por la policía criminal estará siempre sujeta a la confirmación por la autoridad judicial dentro del plazo de 72 horas. 5 - Las incautaciones relacionadas con sistemas informáticos utilizados para la práctica profesional de abogado, médico y la actividad bancaria están sujetos, con las necesarias adaptaciones, a las normas y procedimientos previstos en el Código de Procedimiento Penal, y las relativas a los sistemas informáticos utilizados para ejercer la profesión de periodista, con las necesarias adaptaciones, a las normas y procedimientos previstos en el Estatuto del Periodista. 6 - Se aplica, con las necesarias adaptaciones, el régimen del secreto profesional u oficial y del secreto de Estado, previstos en el artículo 182 del Código de Procedimiento Penal.

	7 - La incautación de datos informáticos, conforme sea más apropiado y proporcionado, teniendo en cuenta los intereses de la causa, podrá adoptar las siguientes formas: a) la incautación del soporte donde está instalado el sistema o la incautación del soporte donde se almacenan los datos informáticos, y los dispositivos necesarios para su lectura; b) hacer una copia de los datos, en soporte autónomo, que se adjuntará al proceso; c) la preservación, por medios tecnológicos, de la integridad de los datos, sin realizar una copia o d) eliminación irreversible o bloqueo del acceso a los datos. 8 - En caso de incautación de acuerdo con el inciso b) anterior, la copia se realizará por duplicado, una de ellas será sellada y encomendada al secretario de los servicios y, si es técnicamente posible, los datos incautados serán certificados por la firma digital. **Artículo 17 - Incautación de comunicaciones electrónicas y de comunicaciones de la misma naturaleza** Cuando, durante un registro informático u otro acceso legítimo a un sistema informático, se encuentren almacenados en ese sistema informático o en otro al que se puede acceder legítimamente mensajes de correo electrónico o registros de comunicaciones de naturaleza similar, el juez podrá autorizar o ordenar la incautación de aquellos que podrían ser de gran interés para establecer la verdad, aplicándose las normas sobre secuestro de de correspondencia del Código de Procedimiento Penal.
Artículo 20 – Obtención en tiempo real de datos relativos al tráfico 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes: a. a obtener o grabar con medios técnicos existentes en su territorio, y b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas: i. a obtener o a grabar con medios técnicos existentes en su territorio, o ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones	**Ley nº 109/2009 (15 de septiembre)** **Artículo 18 - Interceptación de las comunicaciones** 1 - Será admisible la interceptación de las comunicaciones cuando se investiguen los delitos: a) previstos en esta ley, o b) aquellos cometidos por medio de un sistema informático o en los que sea necesario reunir pruebas en formato electrónico, cuando estos delitos se encuentren previstos en el artículo 187 del Código de Procedimiento Penal. 2 - La interceptación de transmisiones de datos informáticos sólo será permitida mientras dure la investigación si hay razones para creer que es esencial para establecer la verdad o para la obtención de pruebas que, de lo contrario, serían

específicas transmitidas en su territorio por medio de un sistema informático. 2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya 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 14 y 15.	imposibles o muy difícil de obtener, mediante orden motivada del juez y previa solicitud del Ministerio Público. 3 - La interceptación puede destinarse al registro de datos sobre el contenido de las comunicaciones o apenas a la recopilación y registro de los datos de tráfico, a lo cual deberá hacer referencia la orden correspondiente, de acuerdo con las necesidades específicas de la investigación. 4 – Para todo lo que no está en contradicción con este artículo, en lo que respecta a la interceptación y el registro de transmisiones de datos informáticos es válido el régimen aplicable a la interceptación y grabación de conversaciones o llamadas telefónicas previstas en los artículos 187, 188 y 190 del Código de Procedimiento Penal.
Artículo 21 – Interceptación de datos relativos al contenido 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a: a. obtener o grabar con medios técnicos existentes en su territorio, y b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a: i. obtener o grabar con 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 relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. 2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en	**Ley nº 109/2009 (15 de septiembre)** **Artículo 18 - Interceptación de las comunicaciones** 1 - Será admisible la interceptación de las comunicaciones cuando se investiguen los delitos: a) previstos en esta ley, o b) aquellos cometidos por medio de un sistema informático o en los que sea necesario reunir pruebas en formato electrónico, cuando estos delitos se encuentren previstos en el artículo 187 del Código de Procedimiento Penal. 2 - La interceptación de transmisiones de datos informáticos sólo será permitida mientras dure la investigación si hay razones para creer que es esencial para establecer la verdad o para la obtención de pruebas que, de lo contrario, serían imposibles o muy difícil de obtener, mediante orden motivada del juez y previa solicitud del Ministerio Público. 3 - La interceptación puede destinarse al registro de datos sobre el contenido de las comunicaciones o apenas a la recopilación y registro de los datos de tráfico, a lo cual deberá hacer referencia la orden correspondiente, de acuerdo con las necesidades específicas de la investigación. 4 – Para todo lo que no está en contradicción con este artículo, en lo que respecta

ese territorio. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya 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 14 y 15.	a la interceptación y el registro de transmisiones de datos informáticos es válido el régimen aplicable a la interceptación y grabación de conversaciones o llamadas telefónicas previstas en los artículos 187, 188 y 190 del Código de Procedimiento Penal.
Sección 3 – Jurisdicción	
Artículo 22 – Jurisdicción 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido: a. en su territorio; o b. a bordo de un buque que enarbole su pabellón; o c. a bordo de una aeronave matriculada según sus leyes; 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. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados. 3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición. 4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno. 5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un	**Ley nº 109/2009 (15 de septiembre)** **Artículo 27 - Aplicación en el espacio de la ley penal portuguesa y jurisdicción de los tribunales portugueses** 1 - Además de las disposiciones del Código Penal en materia de aplicación de la ley penal portuguesa en el espacio, a menos que exista un tratado o acuerdo internacional en contrario, para los efectos de esta ley, el derecho penal portugués se aplicará a los hechos: a) practicados por portugueses, si a los mismos hechos no es aplicable la ley penal de cualquier otro Estado; b) practicados en el beneficio de personas jurídicas establecidas en territorio portugués; c) que físicamente hayan sido practicados en territorio portugués, aunque su objetivo fuera un sistema informático ubicados fuera de dicho territorio; d) dirigidos a sistemas informáticos ubicado en territorio portugués, independientemente del lugar donde esos hechos hayan sido físicamente practicados. 2 - Cuando, de acuerdo a la aplicabilidad del derecho penal portugués, exista competencia simultánea de los tribunales portugueses y los tribunales de otro Estado miembro de la Unión Europea, pudiendo ser iniciado válidamente en ambos el procedimiento penal por los mismos hechos, la autoridad judicial competente utilizará los órganos y mecanismos establecidos en la Unión Europea para facilitar la cooperación entre las autoridades judiciales de los Estados miembros y coordinar sus acciones con el fin de decidir cuál de los dos Estados introduce o da continuación al procedimiento contra los responsables de la infracción a fin de que se centre en apenas uno de ellos. 3 - La decisión de la aceptación o de la transmisión del procedimiento será adoptada por la autoridad judicial competente, teniendo en cuenta, sucesivamente, los siguientes elementos:

presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.	a) el lugar donde ocurrió el crimen; b) la nacionalidad del infractor, y c) el lugar donde el autor material de los hechos fue encontrado. 4 - Se aplicarán a los delitos tipificados en esta ley, las normas generales de competencia de los tribunales establecidas en el Código de Procedimiento Penal. 5 - En caso de duda en cuanto a la jurisdicción local, incluso cuando físicamente no sean los mismos el lugar donde el agente actuó y el lugar donde está físicamente instalado el sistema informático objeto de la acción, la competencia recaerá en el tribunal donde primero se tuvo noticia de los hechos . **CÓDIGO PENAL** **Artículo 4 - Aplicación territorial - principio general** Salvo tratado o convenio internacional en contrario, la ley penal portuguesa se aplicará a los hechos cometidos: a) En el territorio portugués, independientemente de la nacionalidad del agente o b) a bordo de buques o aeronaves portuguesas. **Artículo 5 - Hechos cometidos fuera del territorio portugués** 1 – Salvo tratado o convenio internacional en contrario, la ley penal portuguesa es también aplicable a los actos cometidos fuera del territorio nacional: a) Cuando constituyen crímenes descritos en los artículos 221, 262 a 271, 308 a 321 y 325 a 345; b) En contra portugueses o por portugueses que viven habitualmente en Portugal en el momento de su práctica y se encuentran aquí; c) Cuando constituyen crímenes descritos en los artículos 159 a 161, 171, 172, 175, 176 y 278 a 280, siempre que el agente se encuentre en Portugal y no pueda ser extraditado o entregado como resultado de la aplicación de la orden de detención europea o otro instrumento de la cooperación internacional que obligan al Estado portugués; d) Cuando constituyen crímenes descritos en los artículos 144, 163 y 164, siendo la víctima menor, siempre que el agente se encuentre en Portugal y no pueda ser extraditado o entregado como resultado de la aplicación de la orden de detención europea u otro instrumento de cooperación internacional que obligan al Estado portugués; e) Por portugueses, o por extranjeros contra portugueses, cuando: i) los agentes se encuentran en Portugal;

	ii) también son punibles con arreglo a la ley del lugar donde se les imputan los hechos, a menos que en ese lugar no se pueda ejercer el poder punitivo, y iii) Constituyan delitos que admita extradición y esta no puede ser concedida o sea decidido no entregar el agente en la ejecución de la orden de detención europea u otro instrumento de cooperación internacional que obligan al Estado portugués; f) Para extranjeros que se encuentran en Portugal y cuya extradición fue solicitada allí, cuando constituyan delitos que permiten la extradición y esta no puede ser concedida o sea decidido no entregar el agente en la ejecución de la orden de detención europea o de otro instrumento de cooperación internacional vinculante del Estado portugués; g) Por persona jurídica o en contra de persona jurídica que tenga su sede en territorio portugués. 2 - La ley penal portuguesa es también aplicable a hechos cometidos fuera del territorio nacional que el Estado portugués está obligado a juzgar por tratado o acuerdo internacional. **Artículo 6 - Restricciones a la aplicación de la ley portuguesa** 1 - La aplicación de la ley portuguesa a hechos cometidos fuera del territorio nacional sólo tiene lugar cuando el agente no ha sido juzgado en ese país por estos hechos o si se fugó al cumplimiento total o parcial de la sentencia. 2 - Si bien se aplica la ley portuguesa, en los términos del párrafo anterior, los hechos son juzgados según la ley del país en que se han cometido cuando en realidad esta es más favorable para el agente. La pena se convierte en la que le corresponder en el sistema portugués, o si no hay una correspondencia directa, en la que la ley portuguesa establece para ello. 3 - El régimen del párrafo anterior no se aplicará a los delitos definidos en a) y b) del apartado 1 del artículo anterior. **Artículo 7 - Lugar de práctica del hecho** 1 - El hecho se considera practicado tanto en el lugar donde, en todo o en parte, y cualquier forma de participación, el agente haya actuado o, en el caso de omisión, debería haber actuado como en aquel en que el resultado típico o el resultado no incluidos en el tipo de delito, se produjo.

	2 – En caso de intento, el hecho también se considera practicado en el lugar donde, de acuerdo con la representación del agente, el resultado debería haber sido producido.
Capítulo III – Cooperación internacional	
Artículo 24 – Extradición 1. a. El presente artículo se aplicará a la extradición entre las Partes por 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. b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo. 2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir. 3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos 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.	No fue regulado en ninguna legislación específica, pero resulta de otras normas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición. 6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo 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 las demandas de extradición o de detención provisional, en ausencia de 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.	
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. 2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35. 3. Cada Parte podrá, en caso de urgencia, formular una solicitud de	**Ley nº 109/2009 (15 de septiembre)** **Artículo 20 - Cooperación internacional** Las autoridades nacionales competentes cooperarán con las autoridades extranjeras competentes en las investigaciones o procedimientos relativos a delitos relacionados con los sistemas informáticos o los datos, así como para la obtención de pruebas de un delito en formato electrónico, de acuerdo con las normas sobre transferencia de datos personales contenidos en la Ley nº 67/98 de 26 de octubre.

asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación. 4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal. 5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría 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 que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo. 2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no	No fue regulado en ninguna legislación específica, pero resulta de otras normas.

obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.	
Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables 1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan 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 las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución; b. las autoridades centrales 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 direcciones de las autoridades designadas en aplicación 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 el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida. 4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida: a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.	No se regulado en ninguna legislación en vigor.

5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades. 6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias. 7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente. 8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada. 9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente. b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol). c. Cuando se formule una solicitud en aplicación del apartado a) del presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informará directamente de ello a la Parte requirente. d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas 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 del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al	

Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.	
Artículo 28 – Confidencialidad y restricciones de uso 1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo. 2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones: a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud. 3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla. 4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.	No fue regulado en ninguna legislación específica, pero resulta de otras normas.
Sección 2 – Disposiciones específicas	
Artículo 29 – Conservación rápida de datos informáticos almacenados 1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una	**Ley nº 109/2009 (15 de septiembre)** **Artículo 22 - Preservación y divulgación expeditas de datos informáticos en la cooperación internacional** 1 - Se puede solicitar a Portugal la preservación expedita de datos informáticos almacenados en un sistema informático aquí ubicado, en relación a los delitos definidos en el artículo 11, con el objetivo de presentar una solicitud de asistencia

solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos. 2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse: a. la autoridad que solicita la conservación; b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo; c. los datos informáticos almacenados que deben conservarse y su relación con el delito; d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático; e. la necesidad de la medida de conservación; y f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados. 3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación. 4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal. 5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si: a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses	para la búsqueda, incautación y divulgación de los mismos. 2 - La solicitud especificará: a) la autoridad que solicita la preservación; b) el delito que está siendo investigado, así como un breve resumen de los hechos conexos; c) los datos informáticos que deben conservarse y su relación con el delito; d) toda la información disponible para identificar a la persona responsable de los datos informáticos o la ubicación del sistema informático; e) la necesidad de la preservación, y f) la intención de presentar una solicitud de ayuda para la búsqueda, incautación y difusión de datos. 3 - En la ejecución de una solicitud de autoridad extranjera competente en virtud de los números anteriores, la autoridad judicial competente dará la orden a quién tenga el control o disponibilidad de estos datos, incluido el proveedor de servicios, para que éste los preserve. 4 - La conservación también puede ser ordenada por la *Polícia Judiciária* con previa autorización de la autoridad judicial competente o en caso de urgencia o peligro en el retraso, siendo en este último caso aplicable lo que se dispone en el número 4 del artículo anterior. 5 – La orden de preservación especificará, bajo pena de nulidad: a) la naturaleza de los datos; b) si se conocen, su origen y su destino, y c) el período de tiempo durante el cual los datos deben conservarse hasta un máximo de tres meses. 6 – En cumplimiento de la orden de preservación dirigida hacia él, quien tenga el control o la disponibilidad de estos datos, incluyendo el proveedor de servicios, preservará de inmediato los datos en cuestión por el período especificado, protegiendo y conservando su integridad. 7 - La autoridad judicial competente, o la *Polícia Judiciária* con autorización de aquella autoridad, podrá ordenar la renovación de la medida por períodos sujetos al límite previsto en c) del número 5, siempre que se verifiquen sus requisitos de admisibilidad, hasta un máximo un año. 8 - Cuando sea presentada la solicitud de ayuda contemplada en el número 1, la autoridad judicial competente determinará la preservación de los datos hasta la adopción de una decisión definitiva sobre la solicitud. 9 - Los datos preservados en virtud del presente artículo se concederán únicamente:

esenciales. 6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud. 7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.	a) a la autoridad judicial competente, en la ejecución de la solicitud de ayuda contemplada en el número 1, de la misma manera que podría hacerse en un caso nacional de características similares, como se dispone en los artículos 13 a 17; b) a la autoridad nacional que emitió la orden de preservación, en las mismas condiciones que podrían realizarse en un caso similar nacional, como se dispone en el artículo 13. 10 - La autoridad nacional a quien, en virtud del número anterior, se proporcionan datos de tráfico identificadores de proveedor de servicios y ruta a través de los cuales se hizo la comunicación, rápidamente los comunicará a la autoridad solicitante, de manera que esta autoridad pueda presentar una nueva solicitud de preservación expedita de datos informáticos. 11 - Las disposiciones de los apartados 1 y 2, se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades portuguesas. **Artículo 23 - Motivos de denegación** 1 - La solicitud de preservación o divulgación expedita de datos informáticos será denegada cuando: a) los datos informáticos en cuestión se refieren a un delito político o delito conexo de acuerdo con los conceptos del derecho portugués; b) atenten contra la soberanía, seguridad, orden público u otros intereses de la República Portuguesa, constitucionalmente definidos; c) el Estado requirente no ofrezca adecuadas garantías de protección de los datos personales. 2 - La solicitud de preservación expedita de datos informáticos podrá aún ser denegada si existieren motivos razonables para creer que la ejecución de la subsecuente solicitud de ayuda para fines de búsqueda, incautación y divulgación de tales datos será rechazada por falta de comprobación del requisito de la doble incriminación.
Artículo 30 – Revelación rápida de datos conservados 1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 22 - Preservación y divulgación expeditas de datos informáticos en la cooperación internacional** 1 - Se puede solicitar a Portugal la preservación expedita de datos informáticos almacenados en un sistema informático aquí ubicado, en relación a los delitos definidos en el artículo 11, con el objetivo de presentar una solicitud de asistencia para la búsqueda, incautación y divulgación de los mismos.

2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si: a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.	2 - La solicitud especificará: a) la autoridad que solicita la preservación; b) el delito que está siendo investigado, así como un breve resumen de los hechos conexos; c) los datos informáticos que deben conservarse y su relación con el delito; d) toda la información disponible para identificar a la persona responsable de los datos informáticos o la ubicación del sistema informático; e) la necesidad de la preservación, y f) la intención de presentar una solicitud de ayuda para la búsqueda, incautación y difusión de datos. 3 - En la ejecución de una solicitud de autoridad extranjera competente en virtud de los números anteriores, la autoridad judicial competente dará la orden a quién tenga el control o disponibilidad de estos datos, incluido el proveedor de servicios, para que éste los preserve. 4 - La conservación también puede ser ordenada por la *Polícia Judiciária* con previa autorización de la autoridad judicial competente o en caso de urgencia o peligro en el retraso, siendo en este último caso aplicable lo que se dispone en el número 4 del artículo anterior. 5 – La orden de preservación especificará, bajo pena de nulidad: a) la naturaleza de los datos; b) si se conocen, su origen y su destino, y c) el período de tiempo durante el cual los datos deben conservarse hasta un máximo de tres meses. 6 – En cumplimiento de la orden de preservación dirigida hacia él, quien tenga el control o la disponibilidad de estos datos, incluyendo el proveedor de servicios, preservará de inmediato los datos en cuestión por el período especificado, protegiendo y conservando su integridad. 7 - La autoridad judicial competente, o la *Polícia Judiciária* con autorización de aquella autoridad, podrá ordenar la renovación de la medida por períodos sujetos al límite previsto en c) del número 5, siempre que se verifiquen sus requisitos de admisibilidad, hasta un máximo un año. 8 - Cuando sea presentada la solicitud de ayuda contemplada en el número 1, la autoridad judicial competente determinará la preservación de los datos hasta la adopción de una decisión definitiva sobre la solicitud. 9 - Los datos preservados en virtud del presente artículo se concederán únicamente: a) a la autoridad judicial competente, en la ejecución de la solicitud de ayuda

	contemplada en el número 1, de la misma manera que podría hacerse en un caso nacional de características similares, como se dispone en los artículos 13 a 17; b) a la autoridad nacional que emitió la orden de preservación, en las mismas condiciones que podrían realizarse en un caso similar nacional, como se dispone en el artículo 13. 10 - La autoridad nacional a quien, en virtud del número anterior, se proporcionan datos de tráfico identificadores de proveedor de servicios y ruta a través de los cuales se hizo la comunicación, rápidamente los comunicará a la autoridad solicitante, de manera que esta autoridad pueda presentar una nueva solicitud de preservación expedita de datos informáticos. 11 - Las disposiciones de los apartados 1 y 2, se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades portuguesas. **Artículo 23 - Motivos de denegación** 1 - La solicitud de preservación o divulgación expeditas de datos informáticos es 1 - La solicitud de preservación o divulgación expedita de datos informáticos será denegada cuando: a) los datos informáticos en cuestión se refieren a un delito político o delito conexo de acuerdo con los conceptos del derecho portugués; b) atenten contra la soberanía, seguridad, orden público u otros intereses de la República Portuguesa, constitucionalmente definidos; c) el Estado requirente no ofrezca adecuadas garantías de protección de los datos personales. 2 - La solicitud de preservación expedita de datos informáticos podrá aún ser denegada si existieren motivos razonables para creer que la ejecución de la subsecuente solicitud de ayuda para fines de búsqueda, incautación y divulgación de tales datos será rechazada por falta de comprobación del requisito de la doble incriminación.
Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados 1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de	**Ley nº 109/2009 (15 de septiembre)** **Artículo 24 - Acceso a datos informáticos en la cooperación internacional** 1 - En ejecución de una solicitud de autoridad extranjera competente, la autoridad judicial competente podrá proceder al registro y secuestro y la divulgación de datos almacenados en un sistema informático ubicado en Portugal, relativos a los delitos mencionados en el artículo 11, cuando se trate de una situación en la que

conformidad con el artículo 29. 2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo. 3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos: a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.	las que el registro y secuestro son admisibles en un caso nacional de características similares. 2 - La autoridad judicial competente actuará tan pronto como sea posible, cuando existieran razones para creer que los datos informáticos en cuestión son especialmente vulnerables a su pérdida o modificación, o cuando la cooperación rápida esté prevista en un instrumento internacional aplicable. 3 - Las disposiciones del número 1 se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades portuguesas.
Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público Una Parte podrá, sin autorización de otra: 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.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 25 - Acceso transfronterizo a datos informáticos almacenados de acceso público o con consentimiento** Las autoridades extranjeras competentes, sin previa petición a las autoridades portuguesas, de conformidad con las normas sobre transmisión de los datos personales contenidos en la Ley nº 67/98 de 26 de octubre, podrán: a) acceder a datos informáticos almacenados en un sistema informático ubicado en Portugal, cuando éstos estén a disposición del público; b) recibir o acceder, por medio de un sistema informático ubicado en su territorio, a datos informáticos almacenados en Portugal, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos.
Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico 1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno. 2. 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.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 26 - Interceptación de las comunicaciones en la cooperación internacional** 1- En ejecución de una petición de una autoridad extranjera competente, podrá ser autorizada por un juez la intercepción de transmisiones de datos informáticos realizadas por medio de un sistema informático ubicado en Portugal, sí así se prevé en acuerdo, tratado o convenio internacional y si se trata de situación en la que dicha interceptación está permitida en virtud del artículo 18, en un caso nacional de características similares. 2 - Tiene competencia para recibir las solicitudes de intercepción la *Polícia Judiciária*, que las presentará al Ministerio Público, para que éste los presente al

	juez a cargo de la comarca de Lisboa para la autorización. 3 - La orden de autorización mencionada en el apartado anterior también permitirá la transmisión inmediata de la comunicación al Estado requirente, si tal procedimiento está previsto en acuerdo, tratado o convenio internacional en virtud del cual se presente la solicitud. 4 - Las disposiciones del apartado 1 se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades portuguesas.
Artículo 34 – Asistencia mutua en relación con 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, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.	**Ley nº 109/2009 (15 de septiembre)** **Artículo 26 - Interceptación de las comunicaciones en la cooperación internacional** 1- En ejecución de una petición de una autoridad extranjera competente, podrá ser autorizada por un juez la intercepción de transmisiones de datos informáticos realizadas por medio de un sistema informático ubicado en Portugal, sí así se prevé en acuerdo, tratado o convenio internacional y si se trata de situación en la que dicha interceptación está permitida en virtud del artículo 18, en un caso nacional de características similares. 2 - Tiene competencia para recibir las solicitudes de intercepción la *Polícia Judiciária*, que las presentará al Ministerio Público, para que éste los presente al juez a cargo de la comarca de Lisboa para la autorización. 3 - La orden de autorización mencionada en el apartado anterior también permitirá la transmisión inmediata de la comunicación al Estado requirente, si tal procedimiento está previsto en acuerdo, tratado o convenio internacional en virtud del cual se presente la solicitud. 4 - Las disposiciones del apartado 1 se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades portuguesas.
Artículo 35 – Red 24/7 1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica	**Ley nº 109/2009 (15 de septiembre)** **Artículo 21 - Punto permanente de contacto para la cooperación internacional** 1 - A los fines de la cooperación internacional, para que pueda proporcionar ayuda inmediata con los fines mencionados en el artículo anterior, la *Policía Judiciária* mantendrá una estructura que garantice un punto de contacto disponible en todo momento, las veinticuatro horas del día, los siete días de la semana. 2 - El punto de contacto podrá ser contactado por otros puntos de contacto, con

internos: a. asesoramiento técnico; b. conservación de datos, de conformidad con los artículos 29 y 30; y c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos. 2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado. b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado. 3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.	arreglo a los acuerdos, tratados o convenios a los cuales Portugal está obligado, o en ejecución de protocolos de cooperación internacional con organismos judiciales o policiales. 3 - La asistencia inmediata que ofrece este punto de contacto permanente incluye: a) la prestación de asesoramiento técnico a otros puntos de contacto; b) la preservación expedita de datos en casos de urgencia o peligro en el retraso, en conformidad con el artículo siguiente; c) la recopilación de pruebas para las que tiene jurisdicción en casos de urgencia o de peligro en el retraso; d) la localización de sospechosos y el suministro de información de carácter jurídico en casos de urgencia o de peligro en el retraso; e) la transmisión inmediata al Ministerio Público de las solicitudes referentes a las medidas contempladas en b) y d), fuera de los casos previstos en los mismos, en vista de su pronta ejecución. 4 - Al actuar conforme a lo previsto en b) a d) anteriores, la *Polícia Judiciária* dará noticia inmediata del hecho al Ministerio Público y remitirá el informe del artículo 253 del Código de Procedimiento Penal. **Artículo 29 - Jurisdicción de la *Polícia Judiciária* con respecto a de la cooperación internacional** Las competencias asignadas en esta ley a la *Polícia Judiciária* con el fin de la cooperación internacional serán realizadas por la unidad de organización que investigue los crímenes cometidos bajo esta ley.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	