REPÚBLICA PORTUGUESA

Ley nº 109/2009 (del 15 de septiembre)

Aprueba la Ley del Cibercrimen, adaptando al ordenamiento jurídico interno la Decisión Marco nº 2005/222/JAI, del Consejo, de 24 de febrero, relativa a los ataques contra los sistemas de información, y la Convención sobre el Cibercrimen del Consejo de Europa.

La Asamblea de la República, en virtud del apartado c) del artículo 161º de la Constitución, decreta el siguiente:

CAPÍTULO I
Objeto y definiciones

Artículo 1
Objeto

La presente ley establece las disposiciones penales materiales y procesales, como así también las disposiciones relativas a la cooperación internacional en asuntos penales, relativas al dominio del Cibercrimen y a la obtención de pruebas en soportes electrónicos, adaptando el orden jurídico interno a la Decisión Marco del Consejo nº 2005/222/JAI, del Consejo, de 24 de febrero relativa a los ataques contra los sistemas de información, y adaptando el derecho interno a la Convención sobre el Cibercrimen del Consejo de Europa.

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 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

Disposiciones penales materiales

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 4

Daño relativo a programas u otros datos informáticos

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

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

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 7

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 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.

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.

Artículo 10

Confiscación de bienes

1. El tribunal podrá ordenar la confiscación a favor del Estado de objetos, materiales, equipamientos, o dispositivos que hubieren servido para la práctica de los crímenes previstos en la presente ley, y que pertenezcan a la persona que ha sido condenada por su práctica.

2. En la evaluación, uso, disposición e indemnización por los bienes incautados por la policía criminal que puedan ser confiscados a favor del Estado, se aplicarán las disposiciones del Decreto-Ley nº 11/2007 del 19 de enero.

CAPÍTULO III

Disposiciones procesales

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.

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 13.

Revelación expedita de datos de tráfico.

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 14.

Orden de presentación o acceso a datos

1. 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.
2. 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 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 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.

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 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 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 19

Acciones encubiertas

1 - Se podrá recurrir a la acción encubierta de la Ley nº 101/2001 del 25 de agosto, en la forma prevista en la misma, en el curso de una investigación sobre los delitos siguientes:

a) los previstos en esta ley;

b) los que hayan sido cometidos por medio de un sistema informático, cuando les corresponda, en abstracto, la pena de prisión de máximo superior a cinco

años o, incluso si la pena es menor, de ser dolosos, los delitos contra la libertad sexual y la libre determinación sexual en los casos en el que la victima sea menor o incapaz, la estafa calificada, la estafa informática y en las comunicaciones, la discriminación racial, religiosa o sexual, los delitos económicos y financieros, y los delitos enunciados en el título IV del Código de Derecho de Autor y Derechos Conexos.

2 - Si es necesario el uso de medios y dispositivos informáticos, se observarán en lo que sea aplicable, las normas para la interceptación de las comunicaciones.

CAPÍTULO IV

Cooperación internacional

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.

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 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 22

Preservación y divulgación expedita 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 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 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 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 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 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 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.

CAPÍTULO V

Disposiciones finales y transitorias

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:

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 .

Artículo 28

Régimen general

En todo lo que no contradiga las disposiciones de esta ley se aplicará a los delitos, a las medidas de procedimiento y a la cooperación internacional en materia penal que en ella figuran, respectivamente, las disposiciones del Código Penal, las del Código de Procedimiento Penal y las de la Ley nº 144 / 99, de 31 de agosto.

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.

Artículo 30

Protección de datos personales

El tratamiento de datos personales con arreglo a esta ley se hará de conformidad con las disposiciones de la Ley nº 67/98, de 26 de octubre, siendo aplicables en caso de violación, las disposiciones de su capítulo VI.

Artículo 31

Revocación

Queda revocada la Ley nº 109/91, de 17 de agosto.

Artículo 32

Entrada en vigor

Esta ley entrará en vigor 30 días después de su publicación.

Aprobada el 23 de julio de 2009.

El Presidente de la *Assembleia da República*, Jaime Gama.

Promulgada el 29 de agosto de 2009.

Para ser publicada.

El Presidente de la República, Aníbal Cavaco Silva.

Refrendada el 31 de agosto de 2009.

El Primer Ministro, José Sócrates Carvalho Pinto de Sousa