Version 14 February 2012

Políticas sobre Criminalidad Informática y Legislación en Centro América

- TALLER REGIONAL -

San José, Costa Rica,
Miércoles 7 al viernes 9 de marzo de 2012

Legislación del delito cibernético

Documento de trabajo

1 Artículo 1 – Definiciones

1.1 Disposiciones de la Convención

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;
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.

1.2 Examples

PORTUGAL

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 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.

DOMINICAN REPUBLIC

Artículo 4.- Definiciones
Computadora: Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y/o señales, que realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole, incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma.
Datos: Es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes, como son aquellos cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales electromagnéticas, signos, señales, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos por medio óptico, celular, radioeléctrico, sistemas electromagnéticos o cualquier otro medio útil a tales fines.

ROMANIA, ART. 35 of Romania Law no 161/2003

Art. 35 - (1) For the purpose of the present law, the terms and phrases below have the following meaning:
a) *„computer system*" means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program;
b) *„automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program;
c) *„computer program*" means a group of instructions that can be performed by a computer system in order to obtain a determined result;
d) *„computer data"* are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function;
e) *„a service provider"* is:
1. any natural or legal person offering the users the possibility to communicate by means of a computer system;
2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;
f) *„traffic data"* are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication
g*) "data on the users"* are represented by any information that can lead to identifying a user, including the type of communication and the serviced used, the post address, geographic address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user;
h) *„security measures"* refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users;
i) *„pornographic materials with minors"* refer to any material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual behaviour.

(2) For the purpose of this title, *a person acts without right* in the following situations:
a) is not authorised, in terms of the law or a contract;
b) exceeds the limits of the authorisation;
c) has no permission from the competent natural or legal person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

BARBADOS

"computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function ;
"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function ;
"service provider" means
(a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and
(b) any other entity that processes or stores computer data on behalf of that entity or those users;
"traffic data" means computer data that
(a) relates to a communication by means of a computer system;
(b) is generated by a computer system that is part of a chain of communication; and
(c) shows the origin, destination, route, time, date, size, duration of the communication of the type of underlying services used to generate the data.

GERMANY

While German law does not provide for a definition of a "computer system" other than referring to "data procressing systems" in Section 303b of the German Criminal Code (see Article 5 below), "computer data" are covered (yet not defined) by Section 202a (2) of the Criminal Code (Strafgesetzbuch), 2009 ("**StGB**")[1]:
Section 202a - Data espionage
(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment of not more than three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.
"Service provider" is covered in part by Section 3 of the German Telecommunications Code (Telekommunikationsgesetz), 2010 ("**TKG**") and in part by Section 2 of the German Telecommunications Media Code (Telemediengesetz), 2010 ("**TMG**"):
Section 3 TKG - Definitions
Within the meaning of this law is or are
1. […]
6. "service provider" anyone who, all or part commercially,
    a) provides telecommunication services or
    b) contributes in doing so.

Section 2 TMG - Definitions
Within the meaning of this law

[1] All English versions of German legal texts, though not representing official translations, have been taken from official sources (http://www.gesetze-im-internet.de) except for the Telecommunications Code (TKG), the Telecommunications Media Code (TMG), the Law on Copyright and Neighbouring Rights (UrhG), the Administrative Offenses Act (OWiG) and the Act on International Legal Assistance in Criminal Matters (IRG).

1. a service provider is any natural or legal person, who stores own or alien telecommunication media for usage, or who mediates access for usage; […]
"Traffic data" are covered by Section 3 of the German Telecommunications Code (Telekommunikationsgesetz), 2010 ("**TKG**"):
Section 3 - Definitions
Within the meaning of this law is or are
1. […]
30. "traffic data" such data which is collected, processed or made use of by the supply of a telecommunication service.

1.3 Informe explicativo

Capítulo I – Terminología
Introducción a las definiciones del Artículo 1

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

Artículo 1.a) - Sistema informático

23. A los efectos de este Convenio, un "sistema informático" es un dispositivo que consta de hardware y software cuya función es el tratamiento automatizado de datos digitales. Puede incluir facilidades de entrada (*input*), salida (*output*) y almacenamiento. Puede funcionar en forma independiente o estar conectado a una red con otros dispositivos similares. "Automatizado" significa sin intervención directa de un ser humano; "tratamiento de datos" significa que los datos que se encuentran en un sistema informático son operados mediante la ejecución de un programa informático. Un "programa informático" es un conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar el resultado deseado. Un equipo puede ejecutar diversos programas. Un sistema informático por lo general consta de diferentes dispositivos, diferenciándose entre el procesador o unidad de procesamiento central y los periféricos. Un "periférico" es un dispositivo que realiza ciertas funciones específicas interactuando con la unidad de procesamiento, como puede ser una impresora, una pantalla de video, un dispositivo para leer o escribir CD u otros dispositivos de almacenamiento de datos.
24. Una red es una interconexión entre dos o más sistemas informáticos. Las conexiones pueden ser terrestres (por ej., alámbricas o por cable), inalámbricas (por ej., radioeléctricas, infrarrojas o satelitales), o de ambos tipos. Una red puede estar limitada geográficamente a un área pequeña (redes de área local) o puede abarcar un área extensa (redes de área extensa), y esas redes pueden a su vez estar interconectadas. Internet es una red global que consta de muchas redes interconectadas que utilizan protocolos comunes. Existen también otros tipos de redes, estén o no conectadas a Internet, capaces de transmitir datos informáticos entre sistemas informáticos. Los sistemas informáticos pueden estar conectados a la red como nodos o pueden ser un instrumento para brindar asistencia en la comunicación a través de la red. Lo esencial es el intercambio de datos a través de la red.

Artículo 1.b) - Datos informáticos

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

en el presente Convenio, así como el objeto de la solicitud de una de las medidas de investigación definidas en el presente Convenio.

Artículo 1.c) - Proveedor de servicios

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

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

Artículo 1.d) - Datos relativos al tráfico

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

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

30. La definición enumera de forma exhaustiva las categorías de datos relativos al tráfico que están comprendidos bajo un régimen específico en el presente Convenio: el origen de una comunicación, su destino, la ruta, la hora (GMT), la fecha, el tamaño, la duración y el tipo de servicio subyacente. No todas esas categorías estarán siempre disponibles técnicamente, o podrán ser suministradas por un proveedor de servicios, o serán necesarias para una investigación penal en particular. El "origen" se refiere a un número de teléfono, dirección de Protocolo de Internet (IP), o a una identificación similar de una instalación de comunicaciones a la que un proveedor de servicios presta sus servicios. El "destino" se refiere a una indicación comparable de una instalación de comunicaciones a las que se transmiten las comunicaciones. El término "tipo de servicio subyacente" se refiere al tipo de servicio que está siendo utilizado en la red, por ej., transferencia de archivos, correo electrónico o envío de mensajes instantáneos.

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

2 Artículo 2 – Acceso ilícito

2.1 Disposiciones de la Convención

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.

2.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC,

Art. 6 Sec.1 Derecho Penal Sustantivo : El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.

ROMANIA, Law 161/2003

Art. 42 – (1) The access without right to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years or a fine.
(2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data the punishment is imprisonment from 6 months to 5 years.
(3) Where the act provided in paragraphs 1-2 is committed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.

GERMANY, section 202a (1) StGB
Data espionage

(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment of not more than three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

2.3 Informe explicativo

Acceso ilícito (Artículo 2)
44. El término "acceso ilícito" abarca el delito básico que constituyen las amenazas peligrosas y los ataques a la seguridad (es decir, contra la confidencialidad, la integridad y la disponibilidad) de los sistemas y datos informáticos. La necesidad de protección refleja los intereses de las organizaciones y las personas para manejar, operar y controlar sus sistemas sin interrupciones ni restricciones. La mera intromisión no autorizada, es decir, la "piratería" (*hacking*), el "sabotaje" (*cracking*) o "la intrusión en el ordenador" (*computer trespass*) debería en principio ser ilícita en sí misma. Puede constituir un impedimento para los usuarios legítimos de los datos y sistemas y puede causar alteración o destrucción, lo que implica altos costos de reconstrucción. Dichas intromisiones pueden brindar acceso a datos confidenciales (incluidas las contraseñas y la información relacionada con los sistemas a los que se pretende acceder) y a secretos con respecto al uso del sistema sin efectuar pago o incluso alentar a los piratas informáticos (*hackers*) a cometer formas más peligrosas de delitos informáticos, tales como los delito de fraude o falsificación informáticos.
45. El medio más eficaz de prevenir el acceso no autorizado es, por supuesto, la adopción y el desarrollo de medidas de seguridad eficaces. Sin embargo, una respuesta de amplio alcance debe incluir también la amenaza y el uso de medidas de derecho procesal. La prohibición penal en cuanto al acceso no autorizado puede brindar una protección adicional al sistema y a los datos propiamente dichos y en una primera etapa contra los peligros descritos más arriba.
46. El término "acceso" abarca la entrada a un sistema informático o a alguna parte del mismo (hardware, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados con los contenidos). Sin embargo, no incluye el mero envío de un mensaje de correo electrónico o de un archivo a ese sistema. El término "acceso" incluye el ingreso a otro sistema informático, al que esté conectado a través de redes de telecomunicaciones públicas, o a un sistema informático que esté conectado a la misma red, como una LAN (red de área local) o una Intranet (red interna) que opere en el seno de una organización. No tiene importancia el método de comunicación utilizado (por ej., desde lejos, incluidos los enlaces inalámbricos, o desde una corta distancia).
47. El acto debe también ser cometido de manera "ilegítima". Además de la explicación dada más arriba, este término implica que el acceso autorizado por el propietario o por otro tenedor legítimo del sistema o de parte del mismo no constituye delito (como, por ej., a los fines de efectuar una verificación autorizada o de proteger el sistema informático en cuestión). Por otra parte, no constituye delito el acceder a un sistema informático que permite el acceso libre y abierto del público, ya que tal acceso es "legítimo".
48. La aplicación de instrumentos técnicos específicos puede dar lugar a un acceso conforme al Artículo 2, tal como el acceso a una página web, de manera directa o a través de enlaces de hipertexto, incluidos enlaces ocultos o la aplicación de "*cookies*" o "robots" para ubicar y recuperar información en aras de la comunicación. La aplicación de tales instrumentos no es *per se* "ilegítima". El mantenimiento de un sitio web público implica el consentimiento por parte del propietario del sitio web que cualquier otro usuario de la red podrá acceder al mismo. La aplicación de las herramientas estándar provistas en los protocolos y programas de

comunicación que comúnmente se aplican no es en sí misma "ilegítima", en particular cuando se puede considerar que el tenedor legítimo del sistema al que se accede ha aceptado su aplicación, por ej., en el caso de las '*cookies*' al no rechazar la instalación inicial o por no eliminarla.

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

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

3 Artículo 3 – Interceptación ilícita

3.1 Disposiciones de la Convención

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.

3.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC*, Law 53-07*

Artículo 9.- Interceptación e Intervención de Datos o Señales. El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar desviar grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.

ROMANIA, ART.43 of Romania Law no 161/2003

Art. 43 – (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.
(2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

BARBADOS

7. A person who knowingly and without lawful excuse or justification intercepts by technical means
(a) any transmission to, from or within a computer system that is not available to the public; or
(b) electromagnetic emissions that are carrying computer data from a computer system
is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

GERMANY - German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**"):

Section 202b - Phishing
Whosoever unlawfully intercepts data (section 202a (2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment of not more than two years or a fine, unless the offence incurs a more severe penalty under other provisions.

3.3 Informe explicativo

Interceptación ilícita (Artículo 3)
51. Esta disposición tiene como finalidad proteger el derecho a la privacidad de las comunicaciones de datos. El delito representa una violación de la privacidad de las comunicaciones tradicionales idéntica a la tradicional intervención y grabación de las conversaciones telefónicas orales entre las personas. El derecho a la privacidad de la correspondencia está consagrado en el Artículo 8 de la Convención Europea de Derechos Humanos. El delito establecido conforme al Artículo 3 aplica ese principio a todas las formas de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos.
52. El texto de la disposición ha sido extraído principalmente del delito de "intercepción no autorizada" contenida en la Recomendación (89) 9. En el presente Convenio se deja claro que las comunicaciones involucradas están relacionadas con las "transmisiones de datos informáticos", así como con las radiaciones electromagnéticas, en las circunstancias que se explican a continuación.
53. La interceptación por "medios técnicos" se refiere a escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos, ya sea en forma directa, mediante el acceso y uso del sistema informático, o en forma indirecta, mediante el uso de dispositivos electrónicos para escuchar en forma secreta o de dispositivos para intervenir conversaciones. La interceptación puede implicar también la grabación. El término "medios técnicos" incluye los dispositivos técnicos conectados a las líneas de transmisión, así como también los dispositivos utilizados para obtener y grabar las comunicaciones inalámbricas. Pueden incluir el uso de software, contraseñas y códigos. El requisito de que se utilice un medio técnico es una matización restrictiva destinada a evitar que se establezcan demasiados delitos.
54. El delito se aplica a las transmisiones "no públicas" de datos informáticos. El término "no públicas" matiza la naturaleza del proceso de transmisión (comunicación) y no la naturaleza de los datos transmitidos. Los datos comunicados pueden ser información que esté accesible al público, pero que las partes quieren comunicar de forma confidencial. También puede ocurrir que se desee mantener los datos en secreto con fines comerciales hasta que se pague por el servicio, como es el caso de la televisión de previo pago. Por lo tanto, el término "no pública" no excluye *per se* las comunicaciones que se realizan a través de las redes públicas. Las comunicaciones efectuadas por los empleados, ya sean o no con fines comerciales, que constituyen "transmisiones no públicas de datos informáticos" también están protegidas contra la interceptación sin permiso, en virtud del Artículo 3 (véase, por ej., la Sentencia de la Corte

Europea de Derechos Humanos en el caso Halford contra el Reino Unido, del 25 de junio de 1997, 20.605/92).

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

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

57. La creación de un delito en relación con "las emisiones electromagnéticas" asegurará un alcance más amplio. Las emisiones electromagnéticas pueden ser emitidas por un ordenador durante su funcionamiento. Dichas emisiones no son consideradas como 'datos' de acuerdo con la definición establecida en el Artículo 1. Sin embargo, los datos pueden ser reconstruidos a partir de dichas emisiones. En consecuencia, la interceptación de los datos provenientes de las emisiones electromagnéticas de un sistema informático está incluida como un delito en virtud de este artículo.

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

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

4 Artículo 4 – Ataques a la integridad de los datos

4.1 Disposiciones de la Convención

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.

4.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC, Law 53-07 against cybercrime

Artículo 10.- Daño o Alteración de Datos. El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo.

ROMANIA, ART.44 of Romania Law no 161/2003

Art. 44 – (1) The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence and is punished with imprisonment from 2 to 7 years.
(2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years.
(3) The same punishment as in paragraph (2) shall sanction the unauthorised data transfer by means of a computer data storage medium.

BARBADOS

5. (1) A person who knowingly or recklessly, and without lawful excuse or justification,
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data;
(d) obstructs, interrupts or interferes with any person in the lawful use of data; or
(e) denies access to data to any person entitled to the data;
is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.
(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

GERMANY - German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**"):

Section 303a - Data tampering
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment of not more than two years or a fine.
(2) The attempt shall be punishable.
(3) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

4.3 Informe explicativo

Ataques a la integridad de los datos (Artículo 4)
60. La finalidad de esta disposición es proporcionar a los datos informáticos y a los programas informáticos una protección similar a la que gozan los objetos corpóreos contra la imposición de un daño deliberado. El interés legal protegido en este caso es la integridad y el correcto funcionamiento o utilización de los datos almacenados o de los programas informáticos.
61. En el párrafo 1, los términos que "dañe" y "deteriore" como actos imbricados se refieren en particular a una alteración negativa de la integridad o del contenido de la información de los datos y programas. El "borrar" datos es el equivalente de la destrucción de un objeto corpóreo. Los destruye y los hace irreconocibles. Por "supresión" de datos informáticos se entiende cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al ordenador o al soporte de datos en que fueron almacenados. El término "alteración" se refiere a la modificación de los datos existentes. Por consiguiente, la introducción de códigos maliciosos, tales como virus y caballos de Troya, está incluido en este párrafo, tal como también lo está la modificación resultante de los datos.
62. Los actos antes mencionados son punibles sólo si se cometen de manera "ilegítima". Las actividades comunes inherentes al diseño de las redes o las prácticas comerciales o de operación comunes como, por ej., la verificación o la protección de la seguridad de un sistema informático autorizadas por el dueño o el operador, o la reconfiguración del sistema operativo de un ordenador que tenga lugar cuando el operador de un sistema adquiere un nuevo software (por ej., el software que permite el acceso a Internet que desactiva programas similares instalados previamente), son efectuadas de manera legítima y, en consecuencia, no constituyen un delito conforme a este artículo. La modificación de los datos relativos al tráfico con el fin de facilitar comunicaciones anónimas (por ejemplo, las actividades de los sistemas de redireccionamiento de mensajes de correo electrónico anónimos), o la modificación de datos con el fin de garantizar la seguridad de las comunicaciones (por ej., el cifrado) deberían en principio ser consideradas una forma de protección legítima de la vida privada y, por lo tanto, ser consideradas actividades legítimas. Sin embargo, las Partes tal vez deseen establecer como delito ciertos abusos relacionados con las comunicaciones anónimas, por ejemplo, cuando la información contenida en el encabezamiento del paquete es alterada con el fin de ocultar la identidad del autor del delito.
63. Además, el infractor debe haber actuado de manera "deliberada".

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

5 Artículo 5 – Ataques a la integridad del sistema

5.1 Disposiciones de la Convención

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.

5.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC, Law 53-07 against cybercrime

Artículo 11.- Sabotaje. El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo.

ROMANIA, ART.45 of Romania Law no 161/2003

The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years.

BARBADOS

6. A person who knowingly or recklessly, and without lawful excuse or justification,
(a) hinders the functioning of a computer system by
(i) preventing the supply of electricity, permanently or otherwise, to a computer system;
(ii) causing electromagnetic interference to a computer system;
(iii) corrupting the computer system by any means;
(iv) adding, deleting or altering computer data; or
(b) interferes with the functioning of a computer system or with a person who is lawfully using or operating a computer system is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

GERMANY - German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**"):

Section 303b - Computer sabotage
(1) Whosoever interferes with data processing operations which are of substantial importance to another by

1. committing an offence under section303a (1); or
2. entering or transmitting data (section 202a (2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,

shall be liable to imprisonment of not more than three years or a fine.
(2) If the data processing operation is of substantial importance for anothers business, enterprise or a public authority, the penalty shall be imprisonment of not more than five years or a fine.
(3) The attempt shall be punishable.
(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender

1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
3. through the offence jeopardises the populations supply with vital goods or services or the national security of the Federal Republic of Germany.

(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

5.3 Informe explicativo

Ataques a la integridad del sistema (Artículo 5)
65. La Recomendación núm. (89) 9 considera estos ataques como sabotaje informático. La disposición pretende establecer como delito el obstaculizar de manera deliberada el uso legítimo de los sistemas informáticos incluidos los servicios de telecomunicaciones utilizando o influenciando los datos informáticos. El interés jurídico protegido es el interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto. El texto está redactado en lenguaje neutral de manera tal que se pueda brindar protección a todo tipo de funciones.
66. El término "obstaculización" se refiere a las acciones que interfieren con el correcto funcionamiento del sistema informático. Dicha obstaculización debe efectuarse mediante la introducción, la transmisión, el daño, el borrado, la alteración o la supresión de datos informáticos.
67. La obstaculización debe además ser "grave", a fin de dar lugar a sanción penal. Cada Parte deberá determinar para sí los criterios que deberán cumplirse para que la obstaculización sea considerada "grave". Por ejemplo, una Parte puede exigir que se haya causado un mínimo de daños para que la obstaculización sea considerada grave. Los encargados de redactar el

presente Convenio consideraron como "grave" el envío de datos a un sistema en particular cuando su forma, tamaño o frecuencia produzca un efecto perjudicial significativo en la capacidad que tiene el dueño o el operador para utilizar dicho sistema, o para comunicarse con otros sistemas (por ej., por medio de programas que generen ataques de "denegación del servicio", códigos maliciosos como los virus que impiden o hacen considerablemente más lento el funcionamiento del sistema, o programas que envían enormes cantidades de correo electrónico a un destinatario con el fin de bloquear las funciones de comunicación del sistema).

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

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

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

6 Artículo 6 – Abuso de los dispositivos

6.1 Disposiciones de la Convención

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

6.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC

Artículo 8.- Dispositivos Fraudulentos. El hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

ROMANIA, ART.46 of Romania Law no 161/2003
Art. 43 – (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.
(2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

BARBADOS

8. A person who knowingly or recklessly, and without lawful excuse or justification,
(a) supplies, distributes or otherwise makes available
(i) a device, including a computer programme, that is designed or adapted for the purpose of committing an offence under section 4, 5, 6 or 7; or
(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7; or
(b) has an item mentioned in paragraph *(a)*(i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7 is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

GERMANY - German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**")

Section 202c - Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a (2)), or
2. software for the purpose of the commission of such an offence,

shall be liable to imprisonment of not more than one year or a fine.
(2) Section 149 (2) and (3) shall apply mutatis mutandis.

Section 149 - Preparatory acts
(1) Whosoever prepares to counterfeit money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another

1. plates, frames, type, blocks, negatives, stencils, computer programs or similar equipment which by its nature is suitable for the commission of the offence;
2. paper, which is identical or easy to confuse with the type of paper designated for the production of money or official stamps and especially protected against imitation; or
3. holograms or other elements affording protection against counterfeiting

shall be liable to imprisonment of not more than five years or a fine if he prepared to counterfeit money, otherwise with imprisonment of not more than two years or a fine.
(2) Whosoever voluntarily

1. gives up the commission of the offence prepared for and averts a danger caused by him that others continue to prepare the offence or commit it,or prevents the completion of the offence; and
2. destroys or renders unusable the means for counterfeiting, to the extentthat they still exist and are useful for counterfeiting, or reports their existence to a public authority or surrenders them there,

shall not be liable under subsection (1) above.
(3) If the danger that others continue to prepare or commit the offence is averted, or the completion of the act prevented regardless of the contribution of the offender his voluntary and earnest efforts to achieve this aim shall suffice in lieu of subsection (2) No 1 above.

6.3 Informe explicativo

Abuso de los dispositivos (Artículo 6)
71. Esta disposición establece como delito separado e independiente la comisión deliberada de actos ilícitos específicos con respecto a ciertos dispositivos o datos de acceso que e utilizan mal con el fin de cometer los delitos antes descritos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos. Como la comisión de estos delitos a menudo requiere la posesión de medios de acceso ("herramientas de piratería") o de otras herramientas, existe un fuerte incentivo para adquirirlas con fines delictivos, lo que puede luego llevar a la creación de una especie de mercado negro para su producción y distribución. Con el fin de combatir dichos peligros con mayor eficacia, el derecho penal debería prohibir en su origen los actos específicos que sean potencialmente peligrosos, antes de que se cometan los delitos previstos en los Artículos 2 a 5. En lo que a esto se refiere, esta disposición se basa en desarrollos recientes en el seno del Consejo de Europa (Convenio Europeo sobre la protección jurídica de los servicios de acceso condicional o basados en dicho acceso – STE núm. 178) y de la Unión Europea (Directiva 98/84/CE del Parlamento Europeo y del Consejo*,* de 20 de noviembre de 1998*,* relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso) y las disposiciones pertinentes en algunos países. Un enfoque similar había sido ya adoptado en el Convenio internacional sobre represión de la falsificación de moneda firmado en Ginebra e 1929.
72. El párrafo 1.a).1 establece como delitos la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los Artículos 2 a 5 del presente Convenio. "Distribución" se refiere al acto de enviar datos a terceros, mientras que "la puesta a disposición" se refiere al poner en línea dispositivos para ser utilizados por otras personas. Este término se propone también abarcar la creación o compilación de hipervínculos con el fin de facilitar el acceso a dichos dispositivos. El término "programa informático" incluido en este Artículo se refiere a los programas concebidos, por ej., para alterar o incluso destruir datos o interferir con el funcionamiento de los sistemas, como es el caso de los virus, o programas concebidos o adaptados para lograr acceso a los sistemas informáticos.
73. Quienes redactaron el presente Convenio debatieron largamente si el término "dispositivos" debería restringirse a aquellos diseñados exclusivamente o específicamente para cometer delitos, excluyendo en consecuencia los dispositivos que tienen un uso dual. Se consideró que

este criterio era demasiado limitado. Podría dar lugar a dificultades insuperables en relación con las pruebas necesarias en un procedimiento penal, por lo que la disposición podría resultar prácticamente inaplicable o aplicable sólo en contadas circunstancias. También se rechazó la alternativa de incluir todos los dispositivos, incluso si son producidos y distribuidos de manera legal. En ese caso, únicamente el elemento subjetivo de la intención de cometer un delito informático sería decisivo para imponer un castigo, un enfoque que tampoco ha sido adoptado en el ámbito de la falsificación de monedas. Como un compromiso razonable el Convenio restringe su alcance a los casos en los que los dispositivos son objetivamente concebidos, o adaptados, principalmente con el fin de cometer un delito. Esto excluirá por lo general a los dispositivos de uso dual.

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

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

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

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

78. Debido a diferentes estimaciones respecto de la necesidad de aplicar el delito de "abuso de los dispositivos" a todos los diferentes tipos de delitos informáticos incluidos en los Artículos 2 a 5, el párrafo 3 permite, en base a una reserva (véase el Artículo 42), la posibilidad de restringir el delito en el derecho interno. Sin embargo, todas las Partes están obligadas a tipificar como delito al menos la venta, distribución o puesta a disposición de una contraseña informática o un código de acceso, como lo estipula el inciso ii) del párrafo 1.a).

7 Artículo 7 – Falsificación informática

7.1 Disposiciones de la Convención

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.

7.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC,

Artículo 18.- De la Falsedad de Documentos y Firmas. Todo aquel que falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, será castigado con la pena de uno a tres años de prisión y multa de cincuenta a doscientas veces el salario mínimo.

ROMANIA, ART.48 of Romania Law no 161/2003

Art. 48 – The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used

for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.

GERMANY - German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**")

Section 269 - Forgery of data intended to provide proof
(1) Whosoever for the purposes of deception in legal commerce stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment of not more than five years or a fine.
(2) The attempt shall be punishable.
(3) Section 267 (3) and (4) shall apply mutatis mutandis.

Section 267 - Forgery
(1) Whosoever for the purpose of deception in legal commerce produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be liable to imprisonment of not more than five years or a fine.
(2) The attempt shall be punishable.
(3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender

1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of fraud or forgery;
2. causes major financial loss;
3. substantially endangers the security of legal commerce through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.

(4) Whosoever commits forgery on a commercial basis as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from six months to five years.

7.3 Informe explicativo

Falsificación informática (Artículo 7)
81. La finalidad de este artículo es establecer un delito paralelo al de falsificación de documentos tangibles. Su objetivo es colmar algunas lagunas en el derecho penal en relación con el delito de falsificación tradicional, que requiere la legibilidad visual de las afirmaciones o declaraciones contenidas en un documento y que no se aplica a los datos almacenados electrónicamente. Las manipulaciones de dichos datos con valor probatorio pueden tener las mismas consecuencias graves que los actos de falsificación tradicionales si un tercero se ve así engañado. La falsificación informática implica la creación o la alteración ilegítimas de los datos almacenados de manera tal que adquieran un valor probatorio diferente en el transcurso de transacciones legales, que se basan en la autenticidad de la información contenida en los datos, y es objeto de un engaño. El interés jurídico que se desea proteger es la seguridad y la fiabilidad de los datos electrónicos, que pueden tener consecuencias para las relaciones legales.
82. Cabe señalar que los conceptos de falsificación varían mucho en la legislación interna de los diferentes países. En algunos, el concepto se basa en la autenticidad respecto del autor del documento y en otros está basado en la veracidad de la declaración contenida en el documento. A pesar de ello, se llegó al acuerdo de que el engaño respecto de la autenticidad se refiere, como mínimo, al autor de los datos, independientemente de la exactitud o la veracidad de los contenidos de los mismos. Las Partes pueden ampliar este concepto e incluir en el término "autenticidad" el carácter genuino de los datos.

83. Esta disposición abarca datos que sean equivalentes a un documento de carácter público o privado, que tenga efectos legales. La "introducción" no autorizada de datos correctos o incorrectos produce una situación que se corresponde con la elaboración de un documento falso. Las posteriores alteraciones (modificaciones, variaciones, cambios parciales), borrado (eliminación de datos de un soporte de datos) y supresiones (retención, ocultación de datos) corresponden en general al delito de falsificación de un documento auténtico.
84. La expresión "a efectos legales" se refiere también a las transacciones y documentos legales que son relevantes desde el punto de vista jurídico.
85. La última frase de la disposición permite a las Partes, al aplicar el delito con arreglo a su derecho interno, exigir además que debe existir la intención de engañar o una intención dolosa similar, para que se considere que existe responsabilidad penal.

8 Artículo 8 – Fraude informático

8.1 Disposiciones de la Convención

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,
con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

8.2 Examples

PORTUGAL

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.
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.

DOMINICAN REPUBLIC

Artículo 13.- Robo Mediante la Utilización de Alta Tecnología. El robo, cuando se comete por medio de la utilización de sistemas o dispositivos electrónicos, informáticos, telemáticos o de telecomunicaciones, para inhabilitar o inhibir los mecanismos de alarma o guarda, u otros semejantes; o cuando para tener acceso a casas, locales o muebles, se utilizan los mismos medios o medios distintos de los destinados por su propietario para tales fines; o por el uso de tarjetas, magnéticas o perforadas, o de mandos, o instrumentos para apertura a distancia o cualquier otro mecanismo o herramienta que utilice alta tecnología, se sancionará con la pena de dos a cinco años de prisión y multa de veinte a quinientas veces el salario mínimo.
Artículo 14.- Obtención Ilícita de Fondos. El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y

multa de cien a quinientas veces el salario mínimo.

Párrafo.- Transferencias Electrónica de Fondos. La realización de transferencias electrónicas de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar, se castigará con la pena de uno a cinco años de prisión y multa de dos a doscientas veces el salario mínimo.

Artículo 15.- Estafa. La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo.

Artículo 16.- Chantaje. El chantaje realizado a través del uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de sus componentes, y/o con el propósito de obtener fondos, valores, la firma, entrega de algún documento, sean digitales o no, o de un código de acceso o algún otro componente de los sistemas de información, se sancionará con la pena de uno a cinco años de prisión y multa de diez a doscientas veces el salario mínimo.

ROMANIA, ART.49 of Romania Law no 161/2003

Art. 49 – The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be punished with imprisonment from 3 to 12 years.

GERMANY – German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**")

Section 263a - Computer fraud

(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by in uencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised in uence on the course of the processing shall be liable to imprisonment of not more than five years or a fine.

(2) Section 263 (2) to (7) shall apply mutatis mutandis.

(3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment of not more than three years or a fine.

(4) In cases under subsection (3) above section 149 (2) and (3) shall apply mutatis mutandis.

Section 263 - Fraud

(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by causing or maintaining an error by pretending false facts or by distorting or suppressing true facts shall be liable to imprisonment of not more than five years or a fine.

(2) The attempt shall be punishable.

(3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender

1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery or fraud;
2. causes a major financial loss of or acts with the intent of placing a large number of persons in danger of financial loss by the continued commission of offences of fraud;
3. places another person in financial hardship;
4. abuses his powers or his position as a public official; or
5. pretends that an insured event has happened after he or another have for this purpose set fire to an object of significant value or destroyed it, in whole or in part, through setting fire to it or caused the sinking or beaching of a ship.

(4) Section 243 (2), section 247 and section 248a shall apply mutatis mutandis.

(5) Whosoever on a commercial basis commits fraud as a member of a gang, whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from six months to five years.
(6) The court may make a supervision order (section 68 (1)).
(7) Section 43a and 73d shall apply if the offender acts as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269. section 73d shall also apply if the offender acts on a commercial basis.

8.3 Informe explicativo

Fraude informático (Artículo 8)
86. Con la llegada de la revolución tecnológica, se han multiplicado las oportunidades para cometer delitos económicos como el fraude, incluido el fraude de tarjetas de crédito. Los bienes representados o administrados a través de sistemas informáticos (fondos electrónicos, depósitos) se han convertido en el blanco de manipulaciones del mismo modo que las formas tradicionales de bienes. Estos delitos consisten principalmente en manipulaciones respecto de la introducción de datos, cuando se introducen datos incorrectos en un ordenador, o en manipulaciones respecto de los programas y otras interferencias al procesamiento de los datos. La finalidad de este artículo es establecer como delito toda manipulación indebida realizada en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes.
87. Para garantizar que están cubiertas todas las posibles manipulaciones relevantes, los elementos constitutivos de la "introducción", "alteración", "borrado" o "supresión" mencionados en el Artículo 8.a) se complementan por el acto general de "interferir con el funcionamiento de un programa o sistema informático" en el Artículo 8.b). Los elementos constituyentes de una "introducción", "alteración", "borrado" o "supresión" tienen un significado idéntico al establecido en los artículos anteriores. El Artículo 8.b) abarca actos tales como manipulaciones de los equipos, actos que impiden la impresión y actos que impiden la grabación o el flujo de los datos, o la secuencia en que se ejecutan los programas.
88. Las manipulaciones relacionadas con el fraude informático constituyen un delito si causan a otra persona perjuicio patrimonial directo, pérdida de la posesión de un bien, y si el autor actuó de manera deliberada para obtener de manera ilegítima un beneficio económico para sí mismo o para otra persona. El término "perjuicio patrimonial", que es un concepto amplio, incluye la pérdida de dinero y de cosas tangibles e intangibles que tengan un valor económico.
89. El delito debe ser cometido de forma "ilegítima", y el beneficio económico debe obtenerse de manera ilegítima. Por supuesto, no se pretende incluir en el delito establecido en este artículo aquellas prácticas comerciales comunes legítimas, destinadas a obtener un beneficio económico, ya que las mismas se realizan legítimamente. Por ejemplo, son legítimas las actividades llevadas a cabo en virtud de un contrato válido entre las personas afectadas (por ej., inhabilitar un sitio web a realizar las funciones conferidas en los términos del contrato).
90. El delito debe ser cometido de manera "deliberada". El elemento general de la intención deliberada se refiere a la manipulación o la interferencia de los equipos informáticos que cause un perjuicio patrimonial a un tercero. El delito requiere también la existencia de una intención deliberada específica de índole fraudulenta o dolosa para obtener un beneficio económico o de otro tipo para sí o para otra persona. Así, por ejemplo, no se pretende incluir en el delito establecido por este artículo aquellas prácticas comerciales con respecto a la competencia en el mercado, que pueden causar un perjuicio patrimonial a una persona y beneficiar a otra, pero que no son llevadas a cabo con una intención fraudulenta o dolosa. Por ejemplo, no se pretende establecer como delito el uso de programas que reúnen información para comparar los precios de las compras que se pueden hacer por Internet ("bots"), incluso si no son autorizados por un sitio visitado por el "bot".

9 Artículo 9 – Delitos relacionados con la pornografía infantil

9.1 Disposiciones de la Convención

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 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.

9.2 Examples

PORTUGAL

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.

DOMINICAN REPUBLIC

Artículo 24.- Pornografía Infantil. La producción, difusión, venta y cualquier tipo de comercialización de imágenes o representaciones de un niño, niña o adolescente con carácter pornográfico en los términos definidos en la presente ley, se sancionará con penas de dos a cuatro años de prisión y multa de diez a quinientas veces el salario mínimo.
Párrafo.- **Adquisición y Posesión de Pornografía Infantil**. La adquisición de pornografía infantil por medio de un sistema de información para uno mismo u otra persona, y la posesión intencional de pornografía infantil en un sistema de información o cualquiera de sus componentes, se sancionará con la pena de tres meses a un año de prisión y multa de dos a doscientas veces el salario mínimo.

ROMANIA, ART.51(1) of Romania Law no 161/2003

Art.51 – (1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years and denial of certain rights the production for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material through a computer system, or possession, without right, child pornography material in a computer system or computer data storage medium.

BARBARDOS

13. (1) A person who, knowingly,
(a) publishes child pornography through a computer system; or
(b) produces child pornography for the purpose of its publication through a computer system; or
(c) possesses child pornography in a computer system or on a computer data storage medium for the purpose of publication is guilty of an offence and is liable on conviction on indictment,
(i) in the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or
(ii) in the case of a corporation, to a fine of $200 000.
(2) It is a defence to a charge of an offence under subsection (1)(i) or (ii) if the person establishes that the child pornography was for a *bona fide* research, medical or law enforcement purpose.
(3) For the purposes of subsection (1),
(a) "child pornography" includes material that visually depicts
(i) a minor engaged in sexually explicit conduct; or
(ii) a person who appears to be a minor engaged in sexually explicit conduct; or
(iii) realistic images representing a minor engaged in sexually explicit conduct;
(b) "publish" includes
(i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;
(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(a)*; or
(iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in paragraph *(a)*.

GERMANY - German Criminal Code (Strafgesetzbuch), 2009 ("**StGB**")

Section 184b - Distribution, acquisition and possession of child pornography

(1) Whosoever

1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography)

shall be liable to imprisonment from three months to five years.

(2) Whosoever undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity shall incur the same penalty.

(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of six months to ten years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the child pornography reproduces an actual or realistic activity.

(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment of not more than two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty.

(5) Subsections (2) and (4) above shall not apply to acts that exclusively serve the fulfilment of lawful official or professional duties.

(6) In cases under subsection (3) above section 73d shall apply. Objects to which an offence under subsection (2) or (4) above relates shall be subject to a depriation order. section 74a shall apply.

Section 184c - Distribution, acquisition and possession of juvenile pornography

(1) Whosoever

1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of persons between the ages of fourteen to eighteen years (juvenile pornography)

shall be liable to imprisonment of not more than three years or a fine.

(2) Whosoever undertakes to obtain possession for another of juvernile pornography reproducing an actual or realistic activity shall incur the same penalty.

(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of three months to five years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the juvenile pornography reproduces an actual or realistic activity.

(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment of not more than one year or a fine.The 1st sentence shall not apply to acts of persons related to juvenile pornography produced by them while under eighteen years of age and with the consent of the persons therein depicted.

(5) Section 184b (5) and (6) shall apply mutatis mutandis.

Section 184d - Distribution of pornographic performances by broadcasting, media services or telecommunications services

Whosoever disseminates pornographic performances via broadcast, media services, or telecommunications services shall be liable pursuant to sections 184 to 184c. In cases under section 184 (1) the 1st sentence above shall not apply to dissemination via media services or telecommunications services if it is ensured by technical or other measures that the pornographic performance is not accessible to persons under eighteen years of age.

9.3 Informe explicativo

Título 3 - Delitos relacionados con el contenido

Delitos relacionados con la pornografía infantil (Artículo 9)

91. El Artículo 9 referente a la pornografía infantil tiene como finalidad reforzar las medidas de protección de los menores, incluida su protección contra la explotación sexual, mediante la modernización de las disposiciones del derecho penal con el fin de circunscribir de manera más eficaz la utilización de los sistemas informáticos en relación con la comisión de delitos de índole sexual contra menores.
92. Esta disposición responde a la preocupación de los Jefes de Estado y de Gobierno del Consejo de Europa, expresada en su 21a Cumbre (Estrasburgo, 10 a 11 de octubre de 1997) en su Plan de Acción (punto III.4) y está acorde con la tendencia internacional encaminada a lograr la prohibición de la pornografía infantil, como se evidencia por la reciente adopción del Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía y por la reciente iniciativa de la Comisión Europea relativa a la lucha contra la explotación sexual de los niños y la pornografía (COM2000/854).
93. Esta disposición establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil. La mayoría de los Estados ya han establecido como delito la producción tradicional y la distribución física de pornografía infantil; con todo, debido al creciente uso de Internet como principal instrumento para el comercio de tales materiales, se consideró sin lugar a dudas que era esencial establecer disposiciones específicas en un instrumento jurídico internacional para combatir esta nueva forma de explotación sexual que representa un peligro para los menores. La opinión generalizada es que los materiales y prácticas en línea tales como el intercambio de ideas, fantasías y consejos entre los pedófilos, desempeñan un papel para apoyar, alentar o facilitar los delitos de índole sexual contra los menores.
94. El párrafo 1.a) establece como delito la producción de pornografía infantil con la intención de difundirla a través de un sistema informático. Esta disposición se consideró necesario para luchar contra los peligros descritos anteriormente con respecto a su origen.
95. El párrafo 1.b) establece como delito la "oferta" de pornografía infantil a través de un sistema informático. El término "oferta" se propone abarcar el hecho de pedir a otros que obtengan pornografía infantil. Implica que la persona que ofrece el material puede en realidad proporcionarlo. El término "puesta a disposición" se propone abarcar el hecho de poner en línea pornografía infantil para que sea utilizada por terceros, por ej., mediante la creación de sitios de pornografía infantil. Este párrafo se propone también abarcar la creación o la recopilación de hipervínculos a sitios de pornografía infantil con el fin de facilitar el acceso a dichos sitios.
96. El párrafo 1.c) establece como delito la difusión o la transmisión de pornografía infantil a través de un sistema informático. La "difusión" es la diseminación activa del material. El hecho de enviar pornografía infantil a otra persona a través de un sistema informático estaría comprendido dentro del delito de "transmisión" de pornografía infantil.
97. La expresión "la adquisición, para uno mismo o para otros" en el párrafo 1.d) significa obtener activamente pornografía infantil, por ej., descargándola.
98. La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos, como un disquete o CD-ROM, es considerada delito en el párrafo 1.e). La posesión de pornografía infantil estimula la demanda de dichos materiales. Una manera eficaz de reducir la producción de pornografía infantil es imponer consecuencias penales a la conducta de cada participante que interviene en la cadena desde la producción hasta la posesión.

99. El término “material pornográfico” en el párrafo 2 se rige por las normas nacionales relativas a la clasificación de los materiales como obscenos, incompatibles con la moral pública o similarmente corruptos. Por consiguiente, puede considerarse que los materiales que tienen un mérito artístico, médico, científico o similares características no son pornográficos. La representación visual incluye los datos almacenados en una disquete de o en otro medio electrónico de almacenamiento de datos informáticos que puedan convertirse en imágenes visuales.
100. La expresión “comportamiento sexualmente explícito” abarca por lo menos las siguientes alternativas, tanto en forma real como simulada: a) las relaciones sexuales, ya sea en forma genital-genital, oral-genital, anal-genital u oral-anal, entre menores, o entre un adulto y un menor, del mismo sexo o del sexo opuesto; b) la bestialidad; c) la masturbación; d) los abusos sádicos o masoquistas en un contexto sexual, o e) la exhibición lasciva de los genitales o la zona púbica de un menor. Es indiferente el hecho de que la conducta descrita sea real o simulada.
101. Los tres tipos de materiales definidos en el párrafo 2 a los fines de la comisión de los delitos mencionados en el párrafo 1 abarcan las representaciones de abuso sexual de un niño real (2.a), las imágenes pornográficas que muestran a una persona que parezca un menor adoptando un comportamiento sexualmente explícito (2b), y, finalmente, las imágenes que, si bien "realistas", no implican de hecho la participación de un niño real en un comportamiento sexualmente explícito (2.c). Este última posibilidad incluye las imágenes alteradas, tales como las imágenes modificadas de personas físicas, o incluso generadas totalmente por medios informáticos.
102. En los tres casos previstos en el párrafo 2, los intereses legales que se protegen son ligeramente diferentes. El párrafo 2.a) se centra más directamente en la protección contra el abuso de menores. Los párrafos 2.b) y 2.c) se proponen brindar protección contra comportamientos que, si bien no necesariamente causan daños al “menor” representado en el material, ya que podría no existir un menor real, podrían ser utilizados para alentar o seducir a niños para que participen en dichos actos y, en consecuencia, forman parte de una subcultura que favorece el maltrato de menores.
103. El término "ilegítimo” no excluye las defensas, excusas o principios legales pertinentes similares que eximen a una persona de responsabilidad en circunstancias específicas. Por consiguiente, el término "ilegítimo" permite que una Parte tome en cuenta los derechos fundamentales, tales como la libertad de pensamiento, de expresión y de la vida privada. Por otra parte, una Parte puede establecer una defensa respecto de una conducta relacionada con un "material pornográfico" que tenga un mérito artístico, médico, científico o de similares características. En relación con el párrafo 2.b), la referencia al término "ilegítimo" podría también permitir, por ej., que una Parte pueda decidir que una persona queda eximida de responsabilidad penal si se demuestra que la persona representada no es un menor en el sentido de lo que aquí se dispone.
104. El párrafo 3 define el término "menor" en relación con la pornografía infantil en general, entendiendo como “menor” toda persona menor de 18 años, conforme con la definición de “menor” contenida en la Convención de las Naciones Unidas sobre los Derechos del Niño (Artículo 1). Se consideró que era una importante cuestión de política establecer una norma internacional uniforme con respecto a la edad. Cabe señalar que la edad se refiere al uso de menores (reales o ficticios) como objetos sexuales, y no a la edad necesaria para consentir una relación sexual.
Sin embargo, reconociendo que algunos Estados exigen un límite de edad inferior en su legislación nacional respecto de la pornografía infantil, la última frase del párrafo 3 prevé que las Partes podrán exigir un límite de edad diferente, siempre y cuando no sea inferior a 16 años.
105. Este artículo enumera diferentes tipos de actos ilícitos en relación con la pornografía infantil que, conforme a los Artículos 2 a 8, las Partes están obligadas a tipificar como delito si fueron cometidos de manera “deliberada". Conforme a este criterio, una persona no es responsable a menos que tenga la intención de ofrecer, poner a disposición, distribuir, transmitir, producir o

poseer pornografía infantil. Las Partes pueden adoptar una norma más específica (véase, por ejemplo, la legislación aplicable en la Comunidad Europea en relación con la responsabilidad de los proveedores de servicios), en cuyo caso regirá dicha norma. Por ejemplo, la responsabilidad puede ser impuesta si existe un "conocimiento y control" de la información que es transmitida o almacenada. No es suficiente, por ejemplo, que un proveedor de servicios haya servido de conducto para el material, o albergado un sitio web o sala de noticias que contuviera dicho material, si no existió la intención exigida conforme al derecho interno respecto al caso particular. Por otra parte, un proveedor de servicios no está obligado a verificar conductas para evitar una responsabilidad penal.

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

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

10.1 Disposiciones de la Convención

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.
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.

10.2 Examples

PORTUGAL
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.
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.

DOMINICAN REPUBLIC

Artículo 25.- Delitos Relacionados a la Propiedad Intelectual y Afines. Cuando las infracciones establecidas en la ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

ROMANIA, ART. 139[8] - 139 [9] and art. 143 of Law on copyright no.8/1996

ART. 139[8] - There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the act of making available to the public, including through the Internet or other computer networks, without the consent of the owners of the copyright of protected works, neighbouring rights or sui generis rights of the manufacturers of databases or copies of such protected work, regardless of the form of storage thereof, in such a manner as to allow to the public to access it from anywhere or at anytime individually chosen.

ART. 139[9] - There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the unauthorised reproduction in information systems of computer software in any of the following ways: install, storage, running or execution, display or intranet transmission.

ART. 143 - (1) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of manufacturing, import, distribution or rental, offer, by any means, for sale or rental or possession in view of selling without right devices or components that allow neutralisation of technical measures of protection or that perform services that lead to neutralisation of technical measures of protection or that neutralise such technical measures of protection, including in the digital environment.
(2) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of person whom, without having the consent of the owners of the copyright, and while knowing or should have known that thus is allowing, facilitating, causing or concealing a violation of a right as set forth in this law:
a) removes or modifies from the protected works for commercial purposes any electronic information relating to the applicable regulations on copyright or neighbouring rights,
b) distributes, imports in view of distribution, broadcasts or publicly communicates or makes available to the public, so as to allow access from any place and at any time chosen individually, without right, through digital technology, works or other protected works for which the information existing in electronic form regarding the regulations on copyright or related rights, have been removed or modified without authorisation.

GERMANY - Law on Copyright and Neighbouring Rights, 2007 ("**UrhG**")

Section 106 - Unauthorized Exploitation of Copyrighted Works
(1) Whoever reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, other than in a manner allowed by law and without the right holder's consent, shall be punished with imprisonment for up to three years or a fine.

(2) An attempt shall be punishable.

Section 107 - Unlawful Affixing of Designation of Author

(1) Whoever

1. without the author's consent, affixes a designation of author (section 10 subsection (1)) to the original of a work of fine art or distributes an original bearing such designation,

2. affixes a designation of author (section 10 subsection (1)) on a copy, adaptation or transformation of a work of fine art in such manner as to give to the copy, adaptation or transformation the appearance of an original or distributes a copy, adaptation or transformation bearing such designation,

shall be punished with imprisonment for up to three years or a fine provided the offence is not subject to a more severe penalty under other provisions.

(2) An attempt shall be punishable.

Section 108 - Infringement of Neighboring Rights

(1) Whoever, other than in a manner allowed by law and without the right holder's consent:

1. reproduces, distributes or publicly communicates a scientific edition (section 70) or an adaptation or transformation of such edition;

2. exploits a posthumous work or an adaptation or transformation of such work contrary to section 71;

3. reproduces, distributes or publicly communicates a photograph (section 72) or an adaptation or transformation of a photograph;

4. exploits a performance contrary to section 77 subsection (1) or (2) or section 78 subsection (1);

5. exploits an audio recording contrary to section 85;

6. exploits a broadcast contrary to section 87;

7. exploits a video or video and audio recording contrary to section 94 or section 95 in conjunction with section 94;

8. uses a database contrary to section 87b (1),

shall be punished with imprisonment for up to three years or a fine.

(2) An attempt shall be punishable.

Section 108a - Unlawful Exploitation on a Commercial Basis

(1) Where the person committing the acts referred to in sections 106 to 108 does so on a commercial basis, the penalty shall be imprisonment for up to five years or a fine.

(2) An attempt shall be punishable.

Section 108b - [Unauthorised interference with technical protection measures and information necessary for rights management]

(1) Any person who,

1. with the intention of enabling access to or use of a work protected under this Act or other subject matter protected under this Act, circumvents an effective technical measure without the consent of the right holder, or

2. knowingly without authorisation

a) removes or alters rights management information originating from right holders, if any such information is affixed to a reproduction of a work or other protected subject matter or is published in connection with the public communication of such a work or other protected subject matter, or

(b) disseminates, prepares for dissemination, broadcasts, publicly communicates or makes available to the public a work or other protected subject matter where rights management information has been removed or altered without authorisation

and in so doing has at least recklessly induced, enabled, facilitated or concealed the infringement of copyright or related rights

shall, if the offence was not committed for the exclusive private use of the perpetrator or persons personally associated with the perpetrator or is not related to such use, be punished with imprisonment for no more than one year or a fine.

(2) Punishment shall also be imposed upon any person who, in violation of section 95a subsection (3), produces, imports, disseminates, sells or rents a device, product or component for commercial purposes.
(3) Where the person committing the acts referred to in subsection (1) does so on a commercial basis, the penalty shall be imprisonment for no more than three years or a fine.

10.3 Informe explicativo

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

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

107. Las infracciones de los derechos de propiedad intelectual, en particular del derecho de autor, se cuentan entre los delitos más comunes cometidos por Internet, lo que causa preocupación tanto a los titulares de derechos de autor como a aquellos que trabajan profesionalmente con redes informáticas. La reproducción y difusión a través de Internet de obras que están protegidas, sin la autorización del titular del derecho de autor, son extremadamente frecuentes. Dichas obras protegidas incluyen las obras literarias, fotográficas, musicales, audiovisuales y demás. La facilidad con que se pueden hacer copias no autorizadas gracias a la tecnología digital y la escala de reproducción y de difusión en el contexto de las redes electrónicas hizo necesario incluir disposiciones referentes a las sanciones penales y aumentar la cooperación internacional en este campo.
108. Cada Parte tiene la obligación de tipificar como delito las infracciones deliberadas de los derechos de autor y otros derechos conexos, a veces denominados derechos afines, derivados de los acuerdos enumerados en el Artículo, "cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático". El párrafo 1 establece sanciones penales contra las infracciones de la propiedad intelectual por medio de un sistema informático. La violación de los derechos de autor ya es considerada un delito en la mayoría de los Estados. El párrafo 2 trata de la violación de los derechos afines por medio de un sistema informático.
109. Las infracciones de la propiedad intelectual y de los derechos afines conforme se definen con arreglo al derecho interno de cada Parte y de conformidad con las obligaciones que cada Parte haya contraído respecto de ciertos instrumentos internacionales. Si bien cada Parte tiene la obligación de tipificar como delito esas infracciones, la manera precisa en la cual tales infracciones se definen en la legislación nacional puede variar de un Estado a otro. Sin embargo, las obligaciones relativas a la tipificación como delito en virtud del Convenio cubren solo las infracciones de la propiedad intelectual abordadas de manera explícita en el Artículo 10 y, por lo tanto, excluyen las infracciones de patentes o de marcas comerciales.
110. Con respecto al párrafo 1, los acuerdos a que se hace referencia son el Convenio de Berna para la Protección de las Obras Literarias y Artísticas - Acta de París del 24 de julio de 1971; el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el comercio (ADPIC) y el Tratado de la OMPI sobre Derechos de Autor. Con respecto al párrafo 2, los instrumentos internacionales citados son: la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma, 1961), el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el comercio (ADPIC) y el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Interpretación o Ejecución y Fonogramas. El uso de la expresión "de conformidad con las obligaciones que haya contraído" en ambos párrafos deja en claro que las Partes Contratantes del presente Convenio no están obligadas a aplicar los acuerdos citados en los cuales no sean Parte; además, si una Parte ha formulado una reserva o

declaración permitida en uno de los acuerdos, dicha reserva puede limitar el alcance de su obligación en virtud del presente Convenio.

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

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

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

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

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

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

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

11 Artículo 11 – Tentativa y complicidad

11.1 Disposiciones de la Convención

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.

11.2 Informe explicativo

Título 5 – Otras formas de responsabilidad y de sanción
Tentativa y complicidad (Artículo 11)
118. La finalidad de este artículo es establecer otros delitos relacionados con la tentativa y la complicidad o la instigación de los delitos contemplados en el Convenio. Como se analiza más adelante, no es necesario que una Parte tipifique como delito la tentativa de cometer cada uno de los delitos establecidos en el Convenio.
119. El párrafo 1 exige que las Partes establezcan como delitos penales el acto de ayudar o instigar a la comisión de cualquiera de los delitos previstos en aplicación de los Artículos 2 al 10. Se incurrirá en responsabilidad por brindar ayuda o por complicidad cuando la persona que comete un delito establecido en el Convenio recibe ayuda de otra persona que también tiene la intención de cometer el delito. Por ejemplo, si bien la transmisión de datos relativos a contenidos perjudiciales o a códigos maliciosos a través de Internet requiere la ayuda de los proveedores de servicios como canal de transmisión, no puede recaer responsabilidad en un proveedor de servicios que no tiene la intención de delinquir en virtud de lo dispuesto en esta sección. Así, el proveedor de servicios no está en la obligación de verificar activamente los contenidos para evitar una responsabilidad penal conforme a esta disposición.
120. En cuanto al párrafo 2, relativo a la tentativa, se estimó que algunos de los delitos definidos en el Convenio, o elementos de esos delitos, presentaban dificultades conceptuales (por ejemplo, los elementos consistentes en ofrecer o poner a disposición pornografía infantil). Por otra parte, algunos sistemas jurídicos limitan los delitos en los que la tentativa es sancionada. En consecuencia, sólo se requiere que la tentativa sea tipificada como delito en relación con los delitos establecidos en aplicación de los Artículos 3, 4, 5, 7, 8, 9 1).a) y 9 1).c).
121. Como ocurre con todos los delitos establecidos conforme al Convenio, el delito de tentativa y complicidad o instigación deberá ser cometido de manera deliberada.
122. El párrafo 3 se ha añadido para dar cuenta de las dificultades que puedan tener las Partes respecto de la aplicación del párrafo 2, en vista de la amplia variedad de conceptos contenidos en el derecho interno de los distintos países, a pesar del esfuerzo realizado en el párrafo 2 para eximir ciertos aspectos de la disposición relativa a la tentativa. Una Parte puede declarar que se reserva el derecho de no aplicar el párrafo 2, en todo o en parte. Esto significa que cualquiera de las Partes que formule una reserva con respecto a esa disposición no estará obligada a tipificar como delito la tentativa, o puede elegir los delitos o las partes de los delitos a los cuales se

aplicarán las sanciones penales en relación con la tentativa. La reserva tiene por objeto posibilitar la más amplia ratificación del Convenio, mientras que al mismo tiempo autoriza a las Partes a preservar algunos de sus conceptos jurídicos fundamentales.

12 Artículo 12 – Responsabilidad de las personas jurídicas

12.1 Disposiciones de la Convención

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

12.2. Informe explicativo

Responsabilidad de las personas jurídicas (Artículo 12)
123. El artículo 12 versa sobre la responsabilidad de las personas jurídicas. Es coherente con la tendencia jurídica actual de reconocer la responsabilidad de las personas jurídicas. Tiene como finalidad imponer la responsabilidad a las empresas, asociaciones y personas jurídicas de similares características por las acciones penales llevadas a cabo por una persona que ejerza funciones directivas en su seno, cuando dichas acciones sean llevadas a cabo para beneficio de la persona jurídica. El Artículo 12 también contempla la posibilidad de exigir responsabilidad cuando una persona que ejerza funciones directivas no vigile o controle debidamente a un empleado o representante de la persona jurídica, en caso de que dicha ausencia de vigilancia o de control facilite la comisión por parte de ese empleado o agente de uno de los delitos previstos en aplicación de este Convenio.
124. En virtud del párrafo 1, es necesario que se cumplan cuatro condiciones para que pueda exigirse responsabilidad. En primer lugar, debe haberse cometido uno de los delitos previstos en el presente Convenio. En segundo lugar, el delito debe haber sido cometido en beneficio de la persona jurídica. En tercer lugar, una persona que ejerza funciones directivas debe haber cometido el delito (incluida la complicidad y la instigación). Por "persona que ejerza funciones directivas" se entiende una persona física que tiene un alto cargo en la organización, como un director. En cuarto lugar, la persona que ejerce funciones directivas debe haber actuado basándose en una de las siguientes facultades: un poder de representación de la persona jurídica, una autorización para tomar decisiones en nombre de la persona jurídica, o una autorización para ejercer funciones de control en el seno de la persona jurídica, lo que demuestra que dicha persona física actuó conforme a sus facultades para comprometer la

responsabilidad de la persona jurídica. En síntesis, el párrafo 1 obliga a las Partes a tener la capacidad de exigir responsabilidad a una persona jurídica sólo en el caso de los delitos cometidos por las personas que ejerzan funciones directivas.

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

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

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

13 Artículo 13 – Sanciones y medidas

13.1 Disposiciones de la Convención

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.

13.2. Informe explicativo

Sanciones y medidas (Artículo 13)
128. Este Artículo está estrechamente relacionado con los Artículos 2 a 11, que definen diversos delitos informáticos o delitos relacionados con la informática que deberían estar sujetos a sanciones conforme al derecho penal. De conformidad con las obligaciones impuestas por dichos artículos, esta disposición obliga a las Partes Contratantes a sacar consecuencias de la grave naturaleza de estos delitos al establecer la imposición de sanciones penales "efectivas, proporcionadas y disuasorias" y, en el caso de las personas físicas, la posibilidad de imponer penas de privación de libertad.
129. Las personas jurídicas a las que se exigirá responsabilidad de conformidad con lo dispuesto en el Artículo 12 deberán también estar sujetas a sanciones "efectivas, proporcionadas y disuasorias", que pueden ser de naturaleza penal, civil o administrativa. En virtud del párrafo 2, las Partes Contratantes están obligadas a prever la posibilidad de imponer sanciones pecuniarias a las personas jurídicas.
130. Este Artículo deja abierta la posibilidad de imponer otras sanciones y medidas que reflejen la gravedad de los delitos; por ejemplo, las medidas podrían incluir un mandamiento judicial o una orden de confiscación. Deja a criterio de las Partes la facultad discrecional para crear un sistema de delitos penales y de sanciones que sea compatible con sus respectivos sistemas jurídicos existentes.

14 Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento

14.1 Disposiciones de la Convención

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 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.

14.2 Informe explicativo

Sección 2 - Derecho procesal

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

132. La revolución tecnológica, que incluye la "autopista electrónica", en que numerosas formas de comunicación y servicios están interrelacionadas e interconectadas y comparten medios de transmisión y transporte convencionales, ha alterado la esfera del derecho penal y los procedimientos penales. La constante expansión de la red de comunicaciones abre nuevas puertas para la actividad delictiva por lo que respecta tanto a los delitos tradicionales como a los nuevos delitos tecnológicos. El derecho penal sustantivo no es el único que debe mantenerse al tanto de estos nuevos abusos, ya que también es necesario que lo estén el derecho procesal

penal y las técnicas de investigación. Del mismo modo, se deben adaptar o desarrollar salvaguardias para mantenerse al corriente del nuevo entorno tecnológico y de las nuevas facultades procesales.

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

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

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

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

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

138. Todos los artículos incluidos en esta Sección se he mención a las "autoridades competentes" y a las facultades que deben conferírseles a los fines de llevar a cabo investigaciones o procedimientos penales específicos. En algunos países, solo los jueces tienen la facultad de ordenar o autorizar la obtención o presentación de pruebas, mientras que en otros países los fiscales o los funcionarios encargados de aplicar las leyes tienen las mismas o

similares facultades. Por lo tanto, por "autoridad competente" se entiende un cuerpo encargado del cumplimiento de la ley, ya sea judicial, administrativo o de otra índole, que esté facultado conforme a la legislación de cada país para ordenar, autorizar o llevar a cabo la ejecución de medidas procesales a los fines de obtener o presentar pruebas en relación con investigaciones o procedimientos penales específicos.

15 Artículo 15 – Condiciones y salvaguardias

15.1 Disposiciones de la Convención

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

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

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

15.2 Informe explicativo

Condiciones y salvaguardias (Artículo 15)

145. La instauración, ejecución y aplicación de los poderes y procedimientos previstos en esta Sección del Convenio estarán sometidos a las condiciones y salvaguardias previstas en el derecho interno de cada Parte. Si bien las Partes están obligadas a introducir ciertas disposiciones de derecho procesal en sus leyes nacionales, las modalidades del establecimiento y la aplicación de esos poderes y procedimientos en sus sistemas jurídicos y la aplicación de los poderes y procedimientos en casos específicos estarán sujetas a las leyes y los procedimientos nacionales de cada Parte. Esas leyes y procedimientos internos, tal como se describe más concretamente a continuación, deberán incluir condiciones o salvaguardias, las que pueden ser provistas constitucionalmente, legislativamente, judicialmente o de otra manera. Las modalidades deberían incluir la adición de ciertos elementos como las condiciones y salvaguardias destinados a lograr un equilibrio entre los requisitos de aplicación de la ley y la protección de los derechos y libertades humanas. Como el Convenio se aplica a Partes que tienen diferentes sistemas jurídicos y culturas muy diversas, no es posible especificar en detalle las condiciones y salvaguardias aplicables a cada poder o procedimiento. Las Partes deberán velar por que estas condiciones y salvaguardias brinden la adecuada protección de los derechos y las libertades humanas. Existen algunas normas comunes o salvaguardias mínimas a las que las Partes de este Convenio deben adherir. Estas incluyen las normas o salvaguardias mínimas que se deriven de las obligaciones contraídas por una Parte en virtud de los instrumentos internacionales aplicables en materia de derechos humanos. Estos instrumentos incluyen el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950) y sus Protocolos adicionales núm. 1, 4, 6, 7 y 12 (STE núm. 005[2], 009, 046, 114, 117 y 177), respecto de los Estados europeos que sean Partes en los

[2] El texto del Convenio ha sido modificado de conformidad con las disposiciones del Protocolo núm. 3 (STE núm. 45), que entró en vigor el 21 de septiembre de 1970, del Protocolo núm. 5 (STE núm. 55), que entró en vigor el 20 de diciembre de 1971 y del Protocolo núm. 8 (STE núm. 118), que entró en vigor el 1 de enero de 1990, y ha integrado también el texto del Protocolo núm. 2 (STE núm. 44) que, de conformidad con el artículo 5, párrafo 3, había sido una parte integral del Convenio desde su entrada en vigor el 21 de septiembre de 1970. Todas las disposiciones que se han modificado

mismos. Incluyen también otros instrumentos aplicables en materia de derechos humanos respecto de Estados que se encuentran en otras regiones (por ejemplo, la Convención Americana Sobre Derechos Humanos (1969) y la Carta Africana sobre Derechos Humanos y de los Pueblos (1981), que sean Partes en estos instrumentos, así como también el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966), cuya ratificación es más universal. Además, las leyes de la mayoría de los Estados prevén protecciones similares.

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

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

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

---

o añadido por esos Protocolos han sido sustituidas por el Protocolo núm. 11 (STE núm. 155), a partir de la fecha de su entrada en vigor el 1 de noviembre de 1998. A partir de esa fecha, el Protocolo núm. 9 (STE núm. 140), que entró en vigor el 1 de octubre de 1994, quedó derogado y el Protocolo núm. 10 (STE núm. 146) ha perdido su razón de ser.

16 Artículo 16 – Conservación rápida de datos informáticos almacenados

16.1 Disposiciones de la Convención

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.

16.2 Examples

PORTUGAL
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.

DOMINICAN REPUBLIC

Artículo 53.- Conservación de los Datos. Las autoridades competentes actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

ROMANIA, ART.54 of Romania Law no 161/2003

(1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

BARBADOS

20. (1) Where a police officer satisfies a Judge on the basis of an *ex parte* application that
(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and
(b) there is a risk that the data may be destroyed or rendered inaccessible,
the Judge may make an order requiring the person in control of the computer system to ensure that the data specified in the order be preserved for a period of up to 14 days.
(2) The period may be extended beyond 14 days where, on an *ex parte* application, a Judge authorises an extension for a further specified period of time.

GERMANY - German Code of Criminal Procedure (Strafprozessordnung), 2008 ("**StPO**")

With respect to **computer data**, Article 16 is covered by Sections 94, 95 and 98 StPO.

Section 94 - [Objects Which May Be Seized]

(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95 - [Obligation to Surrender]
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 98 - [Order of Seizure]
(1) Seizure may be ordered only by the judge and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.
(2) An official who has seized an object without a judicial order shall apply for judicial approval within 3 days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a judicial decision. As long as no public charges have been preferred, the decision shall be made by the court of competency pursuant to Section 162 subsection (1). Once public charges have been preferred, the decision shall be made by the court dealing with the matter. The person concerned may also submit the application to the Local Court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.
(3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within 3 days; the objects seized shall be put at its disposal.
(4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The agency making the request shall be entitled to participate. No such request shall be necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.
With respect to **traffic data**, Article 16 is covered by Section 100g StPO.

Section 100g - [Information on Telecommunications Connections]
(1) If certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory,

1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence or
2. has committed a criminal offence by means of telecommunication;

then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.
(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply *mutatis mutandis*. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.

(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.
(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying:

1. the number of proceedings during which measures were implemented pursuant to subsection (1);
2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
4. the number of months elapsed during which telecommunications call data was intercepted, measured from the time the order was made;
5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable.

Section 100a - [Conditions regarding Interception of Telecommunications]
(1) […]
(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.

Section 100b - [Order to Intercept Telecommunications]
(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.
(2) The order shall be given in writing. The operative part of the order shall indicate:

1. where known, the name and address of the person against whom the measure is directed,
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment.
3. the type, extent and duration of the measure specifying the time at which it will be concluded.

(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply *mutatis mutandis*.
(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) […]

16.3 Informe explicativo

Título 2 - Conservación rápida de datos informáticos almacenados

149. Las medidas contenidas en los Artículos 16 y 17 se aplican a los datos almacenados ya obtenidos y conservados por los titulares de los datos, como, por ej., los proveedores de servicios. No se aplican a la obtención en tiempo real y a la conservación de los datos relativos al tráfico en el futuro ni al acceso en tiempo real a los contenidos de las comunicaciones. Estas cuestiones se abordan en el Título 5.

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

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

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

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

154. Algunos Estados tienen leyes que requieren que ciertos tipos de datos, como es el caso de los datos personales en poder de determinados tipos de titulares de datos no sean conservados y que sean borrados si su conservación ya no persigue una finalidad comercial. En la Unión Europea, el

principio general está previsto en la Directiva 95/46/CE y, en el contexto particular del sector de las telecomunicaciones, en la Directiva 97/66/CE. Esas directivas establecen la obligación de eliminar los datos tan pronto como su almacenamiento ya no sea necesario. Sin embargo, los Estados miembros podrán adoptar leyes para establecer excepciones en los casos necesarios con el fin de prevenir, investigar o iniciar acciones respecto de un delito penal. Estas directivas no impiden que los Estados miembros de la Unión Europea establezcan poderes y procedimientos conforme a lo previsto en su derecho interno con el fin de preservar determinados datos para investigaciones específicas.

155. Para la mayoría de los países, la conservación de los datos es una facultad o procedimiento judicial totalmente nuevo en el derecho interno. Es una nueva e importante herramienta de investigación para hacer frente a los delitos informáticos y los delitos relacionados con la informática, especialmente los delitos cometidos a través de Internet. En primer lugar, debido a la volatilidad de los datos informáticos, éstos son fácilmente objeto de manipulaciones y modificaciones. Por lo tanto, valiosas pruebas de un delito pueden desaparecer fácilmente debido a negligencias en el manejo o las prácticas de almacenamiento; a la manipulación o borrado deliberados de los datos con el fin de destruir las pruebas, o a la eliminación sistemática de datos cuya conservación no se requiere por más tiempo. Un método de preservar la integridad de los datos es que las autoridades competentes registren, o accedan de manera similar, y confisquen, o consigan de manera similar, los datos necesarios. Sin embargo, cuando los datos están bajo la custodia de alguien de confianza, tal como una empresa de renombre, la integridad de los datos puede preservarse más rápidamente con una orden de conservación de datos. Para las empresas legítimas, una orden de conservación de datos puede representar también un menor perjuicio para sus actividades normales y su reputación que el efectuar un registro y confiscación en sus instalaciones. En segundo lugar, los delitos informáticos y los delitos relacionados con el uso de los ordenadores son cometidos en gran medida como resultado de la transmisión de comunicaciones a través de un sistema informático. Estas comunicaciones pueden contener contenidos ilegales, tales como pornografía infantil, virus informáticos u otras instrucciones que causen interferencias con los datos o con el correcto funcionamiento del sistema informático, o pruebas de la comisión de otros delitos, tales como el narcotráfico o el fraude. Determinar el origen o el destino de esas comunicaciones pasadas puede contribuir a determinar la identidad de los autores de los delitos. Con el fin de rastrear esas comunicaciones a fin de determinar su origen o destino, es necesario obtener datos relativos al tráfico relacionados con esas comunicaciones pasadas (véase la explicación adicional respecto de la importancia de los datos relativos al tráfico en el Artículo 17 *infra*). En tercer lugar, cuando estas comunicaciones vehiculan contenidos ilícitos o pruebas de una actividad delictiva y los proveedores de servicios conservan copias de dichas comunicaciones como, por ej., los mensajes de correo electrónico, es importante proceder a la conservación de esas comunicaciones a fin de asegurar que no desaparezcan pruebas esenciales. Obtener copias de esas comunicaciones pasadas (por ej., los mensajes de correo electrónico enviados o recibidos que estén almacenados) puede revelar pruebas de un acto delictivo.

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

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

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

17.1 Disposiciones de la Convención

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al 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.

17.2 Examples

PORTUGAL
Ley nº 109/2009 (15 de septiembre)

Artículo 13 - Revelación expedita de los 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.

DOMINICAN REPUBLIC

Artículo 56.- Proveedores de Servicios. Sin perjuicio de lo establecido en el literal b) del artículo 47 de la presente ley, los proveedores de servicio deberán conservar los datos de tráfico, conexión, acceso o cualquier otra información que pueda ser de utilidad a la investigación, por un período mínimo de noventa (90) días. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) creará un reglamento para el procedimiento de obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en un plazo de 6 meses a partir de la promulgación de la presente ley. Dicha normativa deberá tomar en cuenta la importancia de preservación de la prueba, no obstante la cantidad de proveedores envueltos en la transmisión o comunicación.

ROMANIA, ART.54 of Romania Law no 161/2003

Art. 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.

(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

BARBADOS

19. Where a Judge is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify
(a) the Internet service providers; and
(b) the path through which the communication was transmitted.

GERMANY

Covered by Section 100g StPO (see Article 16 above).

17.3 Informe explicativo

Conservación y revelación parcial rápidas de los datos relativos al tráfico (Artículo 17)
165. Este artículo establece obligaciones específicas en relación con la conservación de los datos relativos al tráfico en aplicación del Artículo 16, y establece la revelación rápida de algunos datos relativos al tráfico con el fin de identificar a los proveedores de servicios que estuvieron involucrados en la transmisión de las comunicaciones especificadas. Los "datos relativos al tráfico" se definen en el Artículo 1.
166. La obtención de los datos relativos al tráfico almacenados correspondientes a comunicaciones pasadas puede ser esencial para determinar el origen o el destino de las comunicaciones realizadas, elemento crucial para identificar a las personas que han distribuido, por ej., pornografía infantil, información fraudulenta como parte de un plan fraudulento o virus informáticos, o que han intentado acceder o han accedido ilegalmente a sistemas informáticos, o que han transmitido comunicaciones a un sistema informático causando interferencias, ya sea a los datos contenidos en el sistema o a su correcto funcionamiento. Sin embargo, se debe señalar que en muchos casos esos datos se almacenan sólo por cortos períodos de tiempo; ello puede obedecer a que las leyes de protección de la vida privada prohíben el almacenamiento de dichos datos, o a que las fuerzas del mercado no alientan el almacenamiento de dichos datos por mucho tiempo. Por consiguiente, es importante que se tomen medidas de conservación destinadas a garantizar la integridad de esos datos (véase *supra* la discusión relativa a la conservación).
167. En muchos casos puede estar involucrado en la transmisión de una comunicación más de un proveedor de servicios. Cada proveedor de servicios puede poseer algunos datos relativos al tráfico relacionados con la transmisión de una comunicación específica, que han sido generados y

conservados por ese proveedor de servicios en relación con el tránsito de la comunicación por su sistema o que han sido aportados por otros proveedores de servicios. A veces los datos relativos al tráfico, o al menos algunos tipos de datos relativos al tráfico, se comparten entre los proveedores de servicios involucrados en la transmisión de la comunicación con fines comerciales, de seguridad o técnicos. En tal caso, cualquiera de los proveedores de servicios puede poseer los datos relativos al tráfico que son esenciales para determinar el origen o el destino de la comunicación. Sin embargo, en muchos casos no hay ningún proveedor de servicios que posea la suficiente cantidad de datos esenciales relativos al tráfico para poder determinar el origen real o el destino de la comunicación. Cada uno posee una parte del rompecabezas, y es necesario examinar cada una de estas partes para identificar el origen o el destino de la comunicación.

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

169. Como los datos relativos al tráfico no son revelados a las autoridades encargadas de aplicar las leyes cuando se envía una orden de conservación de datos a un proveedor de servicios (sino que se obtienen o revelan solo más tarde después de que se han tomado otras medidas jurídicas), las autoridades no pueden saber si el proveedor de servicios posee todos los datos esenciales relativos al tráfico o si otros proveedores de servicios participaron en la transmisión de la comunicación. Por consiguiente, este artículo dispone que el proveedor de servicios que recibe una orden de conservación de datos, o una medida similar, revele con prontitud a las autoridades competentes, o a otra persona designada, un volumen suficiente de datos relativos al tráfico que permita a las autoridades competentes identificar tanto a los proveedores de servicios como la vía por la cual se transmitió la comunicación. Las autoridades competentes deberían especificar con claridad el tipo de datos relativos al tráfico que deben ser revelados. La recepción de esa información permitiría a las autoridades competentes determinar si es necesario tomar medidas de conservación respecto de otros proveedores de servicios. De este modo, las autoridades encargadas de la investigación pueden rastrear la comunicación para determinar su origen o su destino, e identificar al autor, o autores, del delito concreto que se investiga. Las medidas que figuran en este Artículo están también sujetas a las limitaciones, condiciones y salvaguardias previstas en los Artículos 14 y 15.

18 Artículo 18 – Orden de presentación

18.1 Disposiciones de la Convención

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;
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.

18.2 Examples

PORTUGAL
Ley nº 109/2009 (15 de septiembre)

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.

DOMINICAN REPUBLIC

Artículo 54 - Facultades del Ministerio Público. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de:
Ordenar a una persona física o moral la entrega de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;

ROMANIA, ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences

(2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, by any person who holds them or from whom they emerge, and such person shall be bound to comply, under paragraph (1).
(3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

BARBADOS

18. (1) Where a Judge is satisfied on the basis of an application by a police officer that specified computer data or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that
(a) a person in control of a computer system produce from the computer system specified computer data or other intelligible output of that data; and
(b) an Internet service provider in Barbados produce information about persons who subscribe to or otherwise use the service.
(2) A person referred to in paragraph *(a)* or *(b)* of subsection (1) who makes an unauthorised disclosure of any information under his control is guilty of an offence and is liable on conviction on indictment,
(a) in the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or
(b) in the case of a corporation, to a fine of $200 000.

GERMANY

Article 18 (1) lit. a is covered by Section 95 of the German Code of Criminal Procedure (Strafprozessordnung), 2008 ("**StPO**")

Section 95 - [Obligation to Surrender]
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.
Article 18 (1) lit. b is covered by Sections 112 and 113 of the German Telecommunications Code (Telekommunikationsgesetz), 2007 ("**TKG**"):

Section 112 - Automated Information Procedure
(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111 subsection (1), first and third sentences, and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated to other telecommunications service providers for further marketing or other use and, with regard to ported numbers, the current carrier portability codes, are also to be included. Section 111 subsection (1), third and fourth sentences, apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that
1. the Federal Network Agency can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany;
2. data can be retrieved using incomplete search data or searches made by means of a similarity function.
The requesting authority is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to ensure by technical and organisational measures that no retrievals can come to his notice.
(2) Information from the customer data files pursuant to subsection (1) shall be provided to
1. the courts and criminal prosecution authorities;
2. federal and state police enforcement authorities for purposes of averting danger;
3. the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act;
4. federal and state authorities for the protection of the Constitution, the Military Counterintelligence Service and the Federal Intelligence Service;
5. the emergency service centres pursuant to section 108 and the service centre for the maritime mobile emergency number 124124;
6. the Federal Financial Supervisory Authority; and
7. the Customs Administration authorities for the purposes set forth in section 2 subsection (1) of the Undeclared Work Act

via central inquiry offices, as stipulated in subsection (4), at all times, insofar as such information is needed to discharge their legal functions and the requests are submitted to the Federal Network Agency by means of automated procedures.
(3) The Federal Ministry of Economics and Technology shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, and with the consent of the German Bundesrat, a statutory order in which the following matters are regulated
1. the essential requirements in respect of the technical procedures for
a) the transmission of requests to the Federal Network Agency;

b) the retrieval of data by the Federal Network Agency from persons with obligations, including the data types to be used for the queries; and
c) transmission by the Federal Network Agency to the requesting authorities of the data retrieved;
2. the security requirements to be observed; and
3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the statutory order,
a) the minimum requirements in respect of the scope of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates;
b) the permitted number of hits to be transmitted to the requesting authority; and
c) the requirements in respect of the erasure of data not needed.
In other respects, the statutory order may also restrict the query facility for the authorities referred to in subsection (2) numbers 5 to 7 to the extent that is required for such authorities. The Federal Network Agency shall determine the technical details of the automated retrieval procedure in a technical directive to be drawn up with the participation of the associations concerned and the authorised bodies and to be brought into line with the state of the art, where required, and published by the Federal Network Agency in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive not later than one year following its publication. In the event of an amendment to the directive, defect-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.
(4) At the request of the authorities referred to in subsection (2), the Federal Network Agency shall retrieve and transmit to the requesting authority the relevant data sets from the customer data files pursuant to subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the competent body, the Federal Network Agency shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year.
(5) The person with obligations according to subsection (1) shall make all such technical arrangements in his area of responsibility as are required for the provision of information under this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the statutory order and the technical directive pursuant to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations.

Section 113 - Manual Information Procedure
(1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent authorities, at their request, without undue delay, with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or regulatory offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Military Counterintelligence Service. The person with obligations pursuant to sentence 1 shall provide information on data by means of which access to terminal equipment or to storage devices or units installed in such equipment or in the network is protected, notably personal identification numbers (PINs) or personal unlocking keys (PUKs), by virtue of an information request pursuant to section 161 subsection (1), first sentence, or section 163 subsection (1) of the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8 subsection (1) of the Federal Act on the Protection of the Constitution, the corresponding provisions of legislation to protect the constitutions of the *Länder*, section 2

subsection (1) of the Federal Intelligence Service Act or section 4 subsection (1) of the Military Counterintelligence Service Act; such data shall not be transmitted to any other public or private bodies. Access to data which are subject to telecommunications privacy shall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information.
(2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 23 of the Court Remuneration and Compensation Act, is determined by the statutory order referred to in section 110 subsection (9). Sentence 2 also applies in those cases in which, under the manual information procedure, merely data are requested which the person with obligations also keeps available for retrieval under the automated information procedure under section 112. Sentence 2 does not apply in those cases in which the information was not provided completely or correctly under the automated information procedure under section 112.

18.3 Informe explicativo

Título 3 - Orden de presentación
Orden de presentación (Artículo 18)

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

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

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

173. Conforme a lo dispuesto en el párrafo 1.a), una de las Partes garantizará que sus autoridades competentes tengan la facultad de ordenar a una persona que se encuentre en su territorio que comunique determinados datos informáticos que obren en su poder o estén bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento de datos. La expresión "obren en su poder o estén bajo su control" se refiere a la posesión física de los datos en cuestión en el territorio de la Parte que imparta la orden y también a situaciones en las cuales la persona no tenga la posesión física de los datos que deben presentarse, pero que dicha persona pueda, no obstante, controlar libremente la presentación de los mismos desde dentro del territorio de la Parte que imparte la orden (por ejemplo, sujeto a los privilegios aplicables, una persona que recibe una orden de presentación de la información almacenada en su cuenta por medio de un servicio de almacenamiento en línea a distancia tiene la obligación de presentar esa información). Al mismo tiempo, la mera capacidad técnica para acceder remotamente a datos almacenados (por ejemplo, la

capacidad que tiene un usuario para acceder a distancia a través de un enlace de red a datos almacenados que no están bajo su control legítimo) no constituye necesariamente "control" con arreglo al significado de esta disposición. En algunos Estados, el concepto denominado "posesión" en derecho abarca la posesión física y constructiva y es lo suficientemente amplio para satisfacer el requisito de que los datos estén "en su poder o bajo su control".

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

174. En función del derecho interno de cada Parte, las condiciones y salvaguardias contempladas en el párrafo 2 de este Artículo pueden excluir datos o información privilegiada. Una Parte podría desear prescribir diferentes términos, diferentes autoridades competentes y diversas salvaguardias en cuanto a la presentación de determinados tipos de datos informáticos o de información sobre los abonados que esté en posesión de ciertas categorías de personas o de proveedores de servicios. Por ejemplo, con respecto a algunos tipos de datos como la información sobre los abonados disponible públicamente, una Parte podría autorizar que dicha orden sea impartida por los agentes encargados de hacer cumplir las leyes cuando en otras situaciones sería necesaria una orden judicial. Por el contrario, en algunas situaciones una Parte podría exigir, o estar obligada a exigir en virtud de salvaguardias respecto de los derechos humanos, que la orden de presentación de información sea impartida únicamente por las autoridades judiciales tratándose de la obtención de ciertos tipos de datos. Las Partes podrían desear restringir la revelación de esos datos a aquellas situaciones en que la orden de presentación de información ha sido impartida por las autoridades judiciales. El principio de proporcionalidad prevé también cierta flexibilidad en relación con la aplicación de la medida, por ejemplo, en muchos Estados, a fin de excluir su aplicación en los casos de menor cuantía.

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

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

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

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

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

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

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

181. Sin embargo, no debería entenderse que este Artículo impone la obligación a los proveedores de servicios para que mantengan registros de sus abonados, ni tampoco exige a los proveedores de servicios que se aseguren de la exactitud de dicha información. Así, un proveedor de servicios no está obligado a registrar la información referente a la identidad de los usuarios de las denominadas tarjetas de prepago para los servicios de telefonía móvil. Tampoco está obligado a verificar la identidad de los abonados o a rechazar el uso de seudónimos por parte de los usuarios de sus servicios.

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

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

19 Artículo 19 – Registro y confiscación de datos informáticos almacenados

19.1 Disposiciones de la Convención

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 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.

19.2 Examples

PORTUGAL
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.
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.

DOMINICAN REPUBLIC

Artículo 54.- Facultades del Ministerio Público.

a) Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes;
b) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte;
j) Recolectar o grabar los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas;

ROMANIA LAW

Art.56 of Law 61/2003 – (1) Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search.
(2) If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can order performing copies that would serve as evidence and that are achieved according to art. 55, paragraph (3).
(3) When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.
(4) The provisions of the Criminal Procedure Code regarding searches at home are applied accordingly.

508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences *(amended by Emergency Ordinance of Government no. 131/2006).*
ART. 16 - (2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, by any person who holds them or from whom they emerge, and such person shall be bound to comply, under paragraph (1).
(3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

BARBADOS

15. (1) Where a magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, the magistrate may issue a warrant authorising any police officer to

enter and search that place, including any computer, using such reasonable force as is necessary.
(2) A warrant issued under this section may authorise a police officer to *(a)* seize any computer, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed;
(b) inspect and check the operation of any computer referred to in paragraph *(a)*;
(c) use or cause to be used any computer referred to in paragraph *(a)* to search any programme or data held in or available to such computer;
(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer into readable and comprehensible format or text, for the purpose of investigating any offence under this Act;
(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;
(f) make and retain a copy of any programme or data held in the computer referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computers.
(3) A warrant issued under this section may authorise the rendering of assistance by an authorised person to the police officer in the execution of the warrant.
(4) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both.
(5) For the purposes of this section, "authorised person" means a person who has the relevant training and skill in computer systems and technology who is identified, in writing, by the Commissioner of Police or a gazetted officer designated by the Commissioner as authorised to assist the police; "encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data; "plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.
16. (1) A police officer executing a warrant in accordance with section 15 is entitled to require a person who is in possession or control of a computer data storage medium or computer system that is the subject of the search to assist him or an authorised person to *(a)* access and use a computer system or computer data storage medium to search any computer data available to or in the system;
(b) obtain and copy computer data referred to in paragraph *(a)*;
(c) use equipment to make copies;
(d) obtain access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence; and
(e) obtain an intelligible output from a computer system in a plain text format that can be read by a person.
(2) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both.
(3) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version.
17. (1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system following a search or a seizure under section 15, the person who made the search shall, at the time of the search or as soon as practicable after the search,

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and *(b)* give a copy of that list to
(i) the occupier of the premises; or
(ii) the person in control of the computer system.
(2) Subject to subsection (3), a police officer or authorised person shall, on request,
(a) permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or
(b) give the person referred to in paragraph *(a)*, a copy of the computer data.
(3) The police officer or authorised person may refuse to give access to or provide copies of computer data referred to in subsection
(2) if he has reasonable grounds for believing that giving the access or providing the copies
(a) would constitute a criminal offence; or
(b) would prejudice
(i) the investigation in connection with which the search was carried out; or
(ii) another investigation connected to the one in respect of which the search was carried out; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

GERMANY

Article 19 (1) and (3) are covered by Sections 94, 95, 102, 103, 105, 161 and 163 of the German Code of Criminal Procedure (Strafprozessordnung), 2008 ("**StPO**"):

Section 94 - [Objects Which May Be Seized]
(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95 - [Obligation to Surrender]
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 102 - [Search in Respect of the Suspect]
A body search, a search of the property and of the private and other premises of a person who, as a perpetrator or as an inciter or accessory before the fact, is suspected of committing a criminal offence, or is suspected of accessoryship after the fact or of obstruction of justice or of handling stolen goods, may be made for the purpose of his apprehension, as well as in cases where it may be presumed that the search will lead to the discovery of evidence.

Section 103 - [Searches in Respect of Other Persons]
(1) Searches in respect of other persons shall be admissible only for the purpose of apprehending the accused or to follow up the traces of a criminal offence or to seize certain objects, and only if certain facts support the conclusion that the person, trace, or object sought is located on the premises to be searched. For the purposes of apprehending an accused who is strongly suspected of having committed an offence pursuant to section 129a, also in conjunction with section 129b subsection (1), of the Criminal Code, or one of the offences designated in this provision, a search of private and other premises shall also be admissible if they are located in a building in which it may be assumed, on the basis of certain facts, that the accused is located.
(2) The restrictions of subsection (1), first sentence, shall not apply to premises where the accused was apprehended or which he entered during the pursuit.

Section 105 - [Search Order; Execution]
(1) Searches may be ordered only by the judge and, in exigent circumstances, also by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Searches pursuant to Section 103 subsection (1), second sentence, shall be ordered by the judge; in exigent circumstances the public prosecution office shall be authorized to order such searches.
(2) Where private premises, business premises, or enclosed property are to be searched in the absence of the judge or the public prosecutor, a municipal official or two members of the community in the district of which the search is carried out shall be called in, if possible, to assist. The persons called in as members of the community may not be police officers or officials assisting the public prosecution office.
(3) If it is necessary to carry out a search in an official building or in an installation or establishment of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such search. The requesting agency shall be entitled to participate. No such request shall be necessary if the search is to be carried out on premises which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 161 - [Information and Investigations]
(1) For the purpose indicated in Section 160 subsections (1) to (3), the public prosecution office shall be entitled to request information from all authorities and to make investigations of any kind, either itself or through the authorities and officials in the police force provided there are no other statutory provisions specifically regulating their powers. The authorities and officials in the police force shall be obliged to comply with the request or order of the public prosecution office and shall be entitled, in such cases, to request information from all authorities.
(2) Where measures pursuant to this statute are only admissible where the commission of particular criminal offences is suspected, personal data that has been obtained as a result of a corresponding measure taken pursuant to another statute may be used as evidence in criminal proceedings without the consent of the person affected by the measure only to clear up one of the criminal offences in respect of which such a measure could have been ordered to clear up the offence pursuant to this statute. Section 100d, subsection (5), number 3 shall remain unaffected.
(3) Personal data obtained in or from private premises by technical means for the purpose of personal protection during a clandestine investigation based on police law may be used as evidence, having regard to the principle of proportionality (Article 13 paragraph (5) of the Basic Law), only after determination of the lawfulness of the measure by the Local Court (Section 162 subsection (1)) in whose district the authority making the order is located; in exigent circumstances a judicial decision is to be sought without delay.

Section 163 - [Duties of the Police]
(1) The authorities and officials in the police force shall investigate criminal offences and shall take all measures may not be deferred, in order to prevent concealment of facts. To this end they shall be entitled to request, and in exigent circumstances to demand, information from all authorities, as well as to conduct investigations of any kind insofar as there are no other statutory provisions specifically regulating their powers.
(2) The authorities and officials in the police force shall transmit their records to the public prosecution office without delay. Where it appears necessary that a judicial investigation be performed promptly, transmission directly to the Local Court shall be possible.
Article 19 (2) is covered Section 110 (3) StPO.

Section 110 - [Examination of Papers]
(1) The public prosecution office and, if it so orders, the officials assisting it (section 152 of the Courts Constitution Act), shall have the authority to examine documents belonging to the person affected by the search.
(2) In all other cases, officials shall be authorized to examine papers found by them only if the holder permits such examination. In all other cases they shall deliver any papers, the

examination of which they deem necessary, to the public prosecution office in an envelope which shall be sealed with the official seal in the presence of the holder.
(3) The examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured; Section 98 subsection (2) shall apply *mutatis mutandis*.

19.3 Informe explicativo

Título 4 – Registro y confiscación de datos informáticos almacenados
Registro y confiscación de datos informáticos almacenados (Artículo 19)

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

185. En el entorno de un allanamiento tradicional en relación con documentos o registros, se trata de reunir pruebas que han sido grabadas o registradas en el pasado en forma tangible, por ej., impresos en papel. Los investigadores proceden al allanamiento e inspeccionan dichos datos registrados, confiscando o secuestrando físicamente el registro tangible. La recogida de datos tiene lugar durante el allanamiento y guarda relación con los datos existentes en ese momento. La condición previa para obtener la autoridad legal para llevar a cabo un allanamiento es la existencia de razones para creer, conforme a lo que establecen las leyes nacionales y las salvaguardias de los derechos humanos, que dichos datos existen en un lugar en particular y que pueden servir de prueba respecto de un delito penal concreto.

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

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

de fácil acceso para dicho sistema. Podrían estar almacenados en un dispositivo conexo de almacenamiento de datos conectado directamente al ordenador o indirectamente a través de sistemas de comunicación, tales como Internet. Ello puede o no requerir nuevas leyes para permitir una extensión del registro hasta llegar al punto en que los datos estén efectivamente almacenados (o la recuperación de los datos de ese sitio en el ordenador que es objeto del registro), o el uso de las facultades tradicionales de allanamiento de una manera más coordinada y expedita en ambos lugares.

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

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

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

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

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

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

194. El Convenio no establece la manera en que se permitirá o llevará a cabo la extensión de un registro. Ello dependerá del derecho interno de cada país. Entre las posibles condiciones cabe destacar algunos ejemplos: facultar a la autoridad judicial o de otro tipo que haya autorizado el registro de un sistema informático específico a que autorice la extensión del registro o el acceso de modo similar a un sistema conectado si tuviera motivos para creer (en la medida en que lo exigen las leyes nacionales y las

salvaguardias de los derechos humanos) que el sistema informático conectado puede contener los datos específicos que se están buscando; facultar a las autoridades encargadas de las investigaciones a extender el registro autorizado, o el acceso de modo similar, de un sistema informático específico a un sistema informático conectado cuando existan motivos similares para creer que los datos específicos que se buscan están almacenados en el otro sistema informático; o ejercer las facultades para proceder al registro, o acceder de manera similar, a ambos lugares en forma coordinada y rápida. En todos los casos, los datos objeto del registro deben estar legalmente accesibles desde el sistema informático inicial o estar disponibles en ese sistema.

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

196. El párrafo 3 dispone que las Partes adoptarán medidas para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 ó 2. Esas medidas incluyen la prerrogativa de confiscar equipos informáticos y dispositivos de almacenamiento de datos. En ciertos casos, por ejemplo, cuando los datos están almacenados en sistemas operativos únicos, por lo que no se pueden copiar, es inevitable confiscar el dispositivo de almacenamiento de los datos en su totalidad. Esto también puede ser necesario cuando es necesario almacenar el dispositivo de almacenamiento de datos a fin de recuperar antiguos datos sobre los que se han grabado posteriormente otros datos pero que, sin embargo, han dejado trazas en el dispositivo de almacenamiento de los datos.

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

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

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

200. El párrafo 4 introduce una medida coercitiva para facilitar el registro y la confiscación de datos informáticos. Aborda del problema práctico de la dificultad para acceder a los datos que se desea obtener como prueba e identificarlos, en vista del volumen de datos que pueden ser tratados y almacenados, el uso de medidas de seguridad y la naturaleza de las operaciones informáticas. Reconoce que puede ser necesario consultar a los administradores de los sistemas, que tienen conocimientos particulares de esos sistemas, para determinar la manera más adecuada de llevar a cabo el registro. Por consiguiente, esta disposición permite a las autoridades competentes obligar a un administrador de sistema a que brinde ayuda, dentro de límites razonables, en cuanto al registro y la confiscación.

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

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

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

204. Quienes redactaron el Convenio debatieron asimismo, en el marco del párrafo 5, si las partes interesadas deberían ser informadas de que se lleva a cabo un procedimiento de registro. En el mundo en línea puede ser menos evidente que se ha procedido a un registro y confiscación (copia) de datos que cuando se lleva a cabo un secuestro en el mundo real, cuando los objetos incautados se decomisan físicamente. El derecho interno de algunas Partes no establece la obligación de notificar tratándose de un allanamiento tradicional. Si el convenio requiriese la notificación del registro de un sistema informático, se crearía una discrepancia con las leyes de esas Partes. Por el contrario, algunas Partes pueden considerar que la notificación es una característica esencial de la medida, destinada a mantener la distinción entre registro y confiscación de datos almacenados en ordenador (que en general no pretende ser una medida subrepticia) e interceptación del flujo de datos (que es una medida subrepticia, véanse los Artículos 20 y 21). Por consiguiente, la cuestión de la notificación dependerá de lo que disponga la legislación nacional. Si las Partes consideran necesario contar con un sistema de notificaciones obligatorias a las personas involucradas, se debería tener presente que las notificaciones pueden perjudicar la investigación. Si existiera dicho riesgo, debería considerarse la posibilidad de aplazar la notificación.

20 Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

20.1 Disposiciones de la Convención

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 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.

20.2 Examples

PORTUGAL
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 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.

DOMINICAN REPUBLIC

Article 54.- Powers of the Public Prosecutor's Office.
k) Invite the service provider to retrieve, extract or record data on a given user, as well as real-time traffic data, by technological means;
l) Intercept telecommunications in real time, in accordance with the procedure set out in Article 192 of the Code of Criminal Procedure for the investigation of all the offences punishable under this law;
Artículo 54.- Facultades del Ministerio Público.
k) Solicitar al proveedor de servicios recolectar, extraer o grabar los datos relativos a un usuario, así como el tráfico de datos en tiempo real, a través de la aplicación de medidas tecnológicas;
l) Realizar la intervención o interceptación de las telecomunicaciones en tiempo real, según el procedimiento establecido en el artículo 192 del Código Procesal Penal para la investigación de todos los hechos punibles en la presente ley;

ROMANIA

ART.54 of Romania Law no 161/2003
Art. 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

GERMANY - German Code of Criminal Procedure (Strafprozessordnung), 2008 ("**StPO**")

Section 100g - [Information on Telecommunications Connections]
(1) If certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory,
1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence or
2. has committed a criminal offence by means of telecommunication;

then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred

to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.
(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply *mutatis mutandis*. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.
(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.
(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying:

1. the number of proceedings during which measures were implemented pursuant to subsection (1);
2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
4. the number of months elapsed during which telecommunications call data was intercepted, measured from the time the order was made;
5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable.

Section 100a - [Conditions regarding Interception of Telecommunications]
(1) […]
(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.

Section 100b - [Order to Intercept Telecommunications]
(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.
(2) The order shall be given in writing. The operative part of the order shall indicate:

1. where known, the name and address of the person against whom the measure is directed,
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment.
3. the type, extent and duration of the measure specifying the time at which it will be concluded.

(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply *mutatis mutandis*.

(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) […]

20.3 Informe explicativo

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

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

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

218. Las comunicaciones informáticas pueden constituir o aportar pruebas respecto de los mismos tipos de delitos. Sin embargo, como la tecnología informática es capaz de transmitir grandes volúmenes de datos, incluidos textos e imágenes visuales y sonoras, también se presta más para la comisión de delitos que impliquen la distribución de contenidos ilegales (por ej., la pornografía infantil). Del mismo modo, como los ordenadores son capaces de almacenar grandes cantidades de datos, a menudo de índole privada, el potencial para causar un perjuicio, ya sea económico, social o personal, puede ser significativo si se interfiere con la integridad de estos datos. Además, como la ciencia de la tecnología informática está basada en el procesamiento de los datos, en cuanto producto final y como parte de su función operativa (por ej., la ejecución de programas informáticos), cualquier interferencia con esos datos puede acarrear efectos desastrosos para el buen funcionamiento de los sistemas informáticos. Cuando ocurre distribución ilegal de pornografía infantil, acceso ilícito a un sistema informático o interferencia con el buen funcionamiento del sistema informático o la integridad de los datos, especialmente a distancia, como por ej., a través de Internet, es necesario y crucial rastrear la ruta de las comunicaciones remontándonos desde la víctima hasta el autor del delito. Por lo tanto, la capacidad para obtener datos relativos al tráfico con respecto a las comunicaciones informáticas es tan importante, si no más, que la relativa a las telecomunicaciones puramente tradicionales. Esta técnica de investigación permite correlacionar la hora, la fecha, el origen y el destino de las comunicaciones efectuadas por el sospechoso con la hora de las intrusiones a los sistemas de las víctimas, identificar a otras víctimas o demostrar vínculos con los cómplices.

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

220. Sujeto a lo dispuesto en el párrafo 2, las Partes están obligadas, en virtud del párrafo 1.a) a garantizar que sus autoridades competentes tengan la capacidad para obtener o registrar datos relativos al tráfico

empleando medios técnicos. El artículo no especifica cómo se han de obtener desde el punto de vista tecnológico, y no se definen obligaciones en términos técnicos.

221. Además, en virtud del párrafo 1.b), las Partes están obligadas a garantizar que sus autoridades competentes están facultadas para obligar a un proveedor de servicios a obtener o registrar datos relativos al tráfico, o de cooperar y ayudar a las autoridades competentes para obtener o grabar esos datos. Esa obligación respecto de los proveedores de servicios es aplicable sólo en la medida en que la obtención o la grabación, o la cooperación y la asistencia, transcurran dentro de los límites de la capacidad técnica existente del proveedor de servicios. El artículo no obliga a los proveedores de servicios a asegurarse de que tienen la capacidad técnica para obtener o grabar esos datos, o para brindar cooperación o asistencia. No requiere que adquieran o desarrollen nuevos equipos, contraten expertos o realicen una costosa reconfiguración de sus sistemas. Sin embargo, si sus sistemas y el personal tienen ya la capacidad técnica necesaria para obtener o grabar esos datos, o para brindar cooperación o asistencia, el artículo exigiría que los proveedores tomaran las medidas necesarias para comprometer esa capacidad. Por ejemplo, el sistema puede estar configurado de cierta manera, o el proveedor de servicios podría disponer ya de los programas informáticos necesarios que hagan posible tomar tales medidas que, por lo general, no se llevan a cabo en el curso de las operaciones normales del proveedor de servicios. El artículo requeriría que el proveedor de servicios comprometiera, o activara, dichas características, como exige la ley.

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

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

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

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

servicios y sus empleados que tengan conocimiento de la interceptación deben cumplir con la obligación de guardar el secreto a fin de que el procedimiento pueda llevarse a cabo de manera eficaz.

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

227. Como se señaló más arriba, por lo general se considera que el interés por el respeto de vida privada menos es menos marcado en lo tocante a la obtención de los datos relativos al tráfico que con respecto a la interceptación de los datos relativos al contenido. Los datos relativos al tráfico que tienen que ver con la hora, la duración y el tamaño de la comunicación revelan poca información personal acerca de una persona o su manera de pensar. Sin embargo, el respeto del derecho a la vida privada puede ser considerado una cuestión más importante por lo que se refiere a los datos sobre el origen o el destino de una comunicación (por ej., los sitios web visitados). La obtención de esos datos puede permitir, en ciertos casos, tener un perfil de los intereses de una persona, de sus asociados y de su contexto social. En consecuencia, las Partes deberían tener en cuenta esas consideraciones al establecer las salvaguardias y los requisitos legales apropiados a la hora de emprender esas medidas, de conformidad con lo dispuesto en los Artículos 14 y 15.

21 Artículo 21 – Interceptación de datos relativos al contenido

21.1 Disposiciones de la Convención

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 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.

21.2 Examples

PORTUGAL
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 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.

DOMINICAN REPUBLIC

Article 54.- Powers of the Public Prosecutor's Office.
d) Order service providers, including Internet service providers, to supply information on any user data they may have in their possession or control ;
Artículo 54.- Facultades del Ministerio Público.
d) Ordenar a un proveedor de servicios, incluyendo los proveedores de servicios de Internet, a suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control ;

ROMANIA

ART.57 of Romania Law no 161/2003, ART. 91[1] (Section V[1]) of the Criminal Procedure Code on audio and video interception and recording of conversations or communications by telephone or by any other electronic means of communication

Art.57 – (1) The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence.
(2) The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.
(3) The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months.
(4) Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken.
(5) The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly.

ART. 91[1] - Conditions and cases of interception and recording of conversations or communications by telephone or by any other electronic means of communication
The interception and recording of conversations or communications by telephone or by any electronic means of communication are performed with the reasoned authorisation of a judge, at the request of the public prosecutor who is conducting or supervising criminal prosecution, under the law, in the event that solid data or clues indicate the preparation or perpetration of a criminal offence for which criminal prosecution is conducted ex officio, and interception and recording are required in order to establish the factual situation or because it would be impossible to identify or locate the participants by any other means or such means would cause much delay to the investigation.
Interception and recording of conversations or communications by telephone or by any electronic means of communication may be authorised for criminal offences against national security, as set forth in the Criminal Code and in other special laws, as well as for criminal offences of drug trafficking, weapons trafficking and trafficking in persons, terrorist acts, money laundering, counterfeiting of currency or other valuables, for the criminal offences set forth in Law No.78/2000 on the Prevention, Detection and Punishment of Acts of Corruption, as subsequently amended and supplemented, and for other serious criminal offences or criminal offences that are perpetrated through means of electronic communication. Para. 1 shall apply accordingly.

Authorisation shall be given for the period of time during which interception and recording is needed, however not for more than 30 days, in private by the president of the court that would be competent to try the case in first instance or of the court of the same rank that has jurisdiction over the prosecution office where the public prosecutor works who is conducting or supervising criminal prosecution. In the absence of the president of the court, the authorisation shall be given by a judge designated by the court president.
Such authorisation may be renewed, either before or after the previous one expires, but under the same conditions and for properly justified reasons. However, each extension may not exceed 30 days.
The total duration of authorised interception and recording, with regard to the same person and the same act may not exceed 120 days.
Recording of conversations between a lawyer and the party whom he is representing or assisting within the proceedings may not be used as evidence unless it contains or leads to the establishment of conclusive and useful data or information regarding the preparation or commission by the lawyer of a criminal offence of those provided in para. 1 and 2.
The public prosecutor ordains immediate cessation of interceptions and recordings before the expiry of the authorisation if the reasons that justified such measures no longer exist, and shall inform about this the law court that issued the authorisation.
At the reasoned request of the injured person, the public prosecutor may request authorisation from the judge to intercept and record conversations or communications by the injured person by telephone or by any electronic means of communication, whatever the nature of the criminal offence under investigation.
Interception and recording of conversations or communications shall be authorised by means of a reasoned order, which must include: the actual clues and facts that justify the measure; the reasons for which it would be impossible to determine the factual situation or to identify or locate the participants by other means or the reasons why the investigation would be very much delayed; the person, the means of communication or the place that is subject to recording; and the period for which interception and recording are authorised.

GERMANY - German Code of Criminal Procedure (Strafprozessordnung), 2008 ("**StPO**")

Section 100a - [Conditions regarding Interception of Telecommunications]
(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if

1. certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, and
2. the offence is one of particular gravity in the individual case as welland
3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success.

(2) Serious criminal offences for the purposes of subsection (1), number 1, are:

1. pursuant to the Criminal Code:

a) crimes against peace, high treason, endangering the democratic Rule of Law, treason and endangering external security pursuant to sections 80 to 82, 84 to 86, 87 to 89 and 94 to 100a;
b) bribery of a member of parliament pursuant to section 108e;
c) crimes against the national defence pursuant to sections 109d to 109h;
d) crimes against public order pursuant to sections 129 to 130;
e) counterfeiting money and official stamps pursuant to sections 146 and 151, in each case in conjunction with section 152, as well as section 152a subsection (3) and section 152b subsections (1) to (4);
f) crimes against sexual self-determination in the cases referred to in sections 176a, 176b, 177 subsection (2), number 2, and section 179 subsection (5), number 2;

g) dissemination, purchase and possession of pornographic writings involving children and involving juveniles, pursuant to section 184b subsections (1) to (3), section 184c subsection (3);
h) murder and manslaughter pursuant to sections 211 and 212;
i) crimes against personal liberty pursuant to sections 232 to 233a, 234, 234a, 239a and 239b;
j) gang theft pursuant to section 244 subsection (1), number 2, and aggravated gang theft pursuant to section 244a;
k) crimes of robbery or extortion pursuant to sections 249 to 255;
l) commercial handling of stolen goods, gang handling of stolen goods and commercial gang handling of stolen goods pursuant to sections 260 and 260a;
m) money laundering or concealment of unlawfully acquired assets pursuant to section 261 subsections (1), (2) and (4);
n) fraud and computer fraud subject to the conditions set out in section 263 subsection (3), second sentence, and in the case of section 263 subsection (5), each in connection with section 263a subsection (2);
o) subsidy fraud subject to the conditions set out in section 264 subsection (2), second sentence, and in the case of section 264 subsection (3), in conjunction with section 263 subsection (5);
p) criminal offences involving falsification of documents under the conditions mentioned in section 267 subsection (3), second sentence, and in the case of section 267 subsection (4), in each case also in conjunction with section 268 subsection (5) or section 269 subsection (3), as well as pursuant to sections 275 subsection (2) and section 276 subsection (2);
q) bankruptcy subject to the conditions set out in section 283a, second sentence;
r) crimes against competition pursuant to section 298 and, subject to the conditions set out in section 300, second sentence, pursuant to section 299;
s) crimes endangering public safety in the cases referred to in sections 306 to 306c, 307 subsections (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314, 315 subsection (3), section 315b subsection (3), as well as sections 361a and 361c;
t) taking and offering a bribe pursuant to sections 332 and 334;

2. pursuant to the Fiscal Code

a) tax evasion under the conditions listed in section 370 subsection (3), second sentence, number 5;
b) commercial, violent and gang smuggling pursuant to section 373;
c) handling tax-evaded property as defined in section 374 subsection (2);

3. pursuant to the Pharmaceutical Products Act:

criminal offences pursuant to section 95 subsection (1), number 2a, subject to the conditions listed in section 95 subsection (3), second sentence, number 2b;

4. pursuant to the Asylum Procedure Act:

a) inducing an abusive application for asylum pursuant to section 84 subsection (3);
b) commercial and gang inducement to make an abusive application for asylum pursuant to section 84a;

5. pursuant to the Residence Act:

a) smuggling of aliens pursuant to section 96 subsection (2);
b) smuggling resulting in death and commercial and gang smuggling pursuant to section 97; pursuant to the Foreign Trade and Payments Act:
criminal offences pursuant to section 34 subsections (1) to (6);

6. pursuant to the Narcotics Act:

a) criminal offences pursuant to one of the provisions referred to in section 29 subsection (3), second sentence, number 1, subject to the conditions set out therein;
b) criminal offences pursuant to sections 29a, 30 subsection (1), numbers 1, 2 and 4, as well as sections 30a and 30b;

7. pursuant to the Precursors Control Act:

criminal offences pursuant to section 19 subsection (1), subject to the conditions set out in section 19 subsection (3), second sentence;

8. pursuant to the War Weapons Control Act:

a) criminal offences pursuant to section 19 subsections (1) to (3) and section 20 subsections (1) and (2), as well as section 20a subsections (1) to (3), each also in conjunction with section 21;
b) criminal offences pursuant to section 22a subsections (1) to (3);

9. pursuant to the Code of Crimes against International Law:

a) genocide pursuant to section 6;
b) crimes against humanity pursuant to section 7;
c) war crimes pursuant to sections 8 to 12;

10. pursuant to the Weapons Act:

a) criminal offences pursuant to section 51 subsections (1) to (3);
b) criminal offences pursuant to section 52 subsection (1) numbers 1, 2c and 2d, as well as section 52 subsections (5) and (6).

(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.
(4) If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented.

Section 100b - [Order to Intercept Telecommunications]

(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.
(2) The order shall be given in writing. The operative part of the order shall indicate:

1. where known, the name and address of the person against whom the measure is directed,
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment.
3. the type, extent and duration of the measure specifying the time at which it will be concluded.

(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply *mutatis mutandis*.
(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) The *Länder* and the Federal Public Prosecutor General shall submit a report to the Federal Office of Justice every calendar year by the 30th June of the year following the reporting year, concerning measures ordered pursuant to Section 100a within their area of competence. The Federal Office of Justice shall produce a summary of the measures ordered nationwide during the reporting year and shall publish it on the Internet.
(6) The reports pursuant to subsection (5) shall indicate:

1. the number of proceedings in which measures were ordered pursuant to Section 100a subsection (1);

2. the number of orders to intercept telecommunications pursuant to Section 100a subsection (1), distinguishing between

a) initial and follow-up orders, as well as

b) fixed, mobile and Internet telecommunication;

in each case the underlying criminal offence by reference to the categories listed in Section 100a subsection (2).

21.3 Informe explicativo

Interceptación de datos relativos al contenido (Artículo 21)

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

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

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

231. Además, como se indica en las observaciones anteriores sobre el Artículo 20, las condiciones y salvaguardias aplicables a la interceptación en tiempo real de datos relativos al contenido pueden ser más rigurosas que las aplicables a la obtención en tiempo real de datos relativos al tráfico, o al registro y confiscación, o al acceso por medios similares, de los datos almacenados.

Capítulo III – Cooperación internacional

29 Artículo 29 – Conservación rápida de datos informáticos almacenados

29.1 Disposiciones de la Convención

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 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 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.

29.2 Examples

PORTUGAL
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 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.

ROMANIA, ART.63 of Romania Law no 161/2003

Art. 63 - (1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal matters.
(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
a) the authority requesting the preservation;
b) a brief presentation of facts that are subject to the criminal investigation and their legal background;
c) computer data required to be preserved;
d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;
e) the utility of the computer data and the necessity to preserve them;
f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;
(3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters;

GERMANY
Article 29 is covered by Sections 66 and 67 of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("**IRG**") in the absence of applicable international agreements:

Section 66 - Surrender of objects
(1) Upon request by the competent authority of a foreign country, objects may be surrendered
1. which may serve as evidence for foreign proceedings or
2. which the person concerned or a participant acquired as a result of the offence on which the request is based or as consideration for such objects.
(2) Surrender shall be admissible only if
1. the act giving rise to the request constitutes an unlawful act also under German law which fulfils the elements of an offence contained in a penal act or an act which permits punishment by non-criminal fine, or if it would constitute such an act also under German law if the facts were transposed to an analogous context,
2. a seizure order issued by a competent authority of the requesting state has been submitted or such an authority has made a declaration stating that the requirements for seizure would be fulfilled if the objects were located in the requesting state, and
3. an assurance is given that the rights of third parties will remain unaffected and that objects surrendered subject to reservation will be returned immediately upon request.

(3) The public prosecution office at the Regional Court shall prepare the decision on surrender and carry out surrender once it has been authorised. The public prosecution office at the Regional Court in whose region the objects are located shall have local jurisdiction. Section 61 subsection (2), second sentence, shall apply accordingly.

Section 67 - Search and seizure
(1) Objects that may become the subject of surrender to a foreign state may be seized or otherwise secured even prior to the receipt of the request for surrender. A search may also be conducted for this purpose.
(2) Subject to the conditions set forth in section 66 subsection (1) number 1 and subsection (2) number 1, objects may also be seized or otherwise secured if necessary for the execution of a request which is not directed toward the surrender of the objects. Subsection (1), second sentence, shall apply accordingly.
(3) The search and seizure shall be ordered by the Local Court in whose district the actions are to be conducted. Section 61 subsection (2), second sentence, shall apply accordingly.
(4) In case of imminent danger, the public prosecution office and its investigative personnel (section 152 of the Courts Constitution Act) shall be authorised to order the search and seizure.

29.3 Informe explicativo

Título 1 - Asistencia mutua en materia de medidas provisionales
Conservación rápida de datos informáticos almacenados (Artículo 29)
282. Este artículo establece un mecanismo a nivel internacional equivalente al prevista en el Artículo 16 para su uso a nivel nacional. El párrafo 1 de este Artículo autoriza a una Parte a hacer una solicitud (y el párrafo 3 establece que cada Parte debe tener la capacidad legal para obtener) la conservación rápida de datos almacenados en el territorio de la Parte requerida por medio de un sistema informático, con el fin de que los datos no sean alterados, retirados o eliminados durante el período de tiempo necesario para preparar, transmitir y ejecutar una solicitud de asistencia mutua para obtener los datos. La conservación es una medida limitada y provisional, concebida para ser aplicada mucho más rápidamente que la ejecución de una solicitud tradicional de asistencia mutua. Como ya se ha indicado previamente, los datos informáticos son muy volátiles. Con unas pocas pulsaciones, o mediante la operación de programas automáticos, pueden ser eliminados, alterados o trasladados, lo que hace imposible seguir la pista de un delito hasta su autor o destruyendo pruebas esenciales de su culpabilidad. Algunas formas de datos informáticos están almacenados sólo por cortos períodos de tiempo antes de ser eliminados. Por ello, se acordó que era necesario contar con un mecanismo para asegurar la disponibilidad de dichos datos, que dependían del proceso mucho más largo y complicado de ejecutar una solicitud formal de asistencia mutua, lo que puede tomar semanas o meses.
283. Si bien es mucho más rápida que la práctica convencional de asistencia mutua, esta medida es al mismo tiempo menos intrusiva. Los funcionarios encargados de la asistencia mutua de la Parte requerida no están obligados a obtener la posesión de los datos de quien los custodia. El procedimiento preferido es que la Parte requerida asegure que el custodio de los datos (con frecuencia, un proveedor de servicios u otro tercero) preservará (es decir, no eliminará) los datos hasta que se lleve a cabo el proceso que requiere que los mismos sean entregado a los agentes del orden en una etapa posterior. Este procedimiento tiene la ventaja de ser rápido y de proteger la intimidad de la persona a la que corresponden los datos, ya que éstos no serán revelados ni examinados por ningún funcionario gubernamental hasta que se cumplan los criterios estipulados para permitir la revelación plena de los mismos conforme a los regímenes normales de asistencia mutua habituales. Al mismo tiempo, la Parte requerida puede utilizar otros procedimientos para asegurar la conservación rápida de los datos, incluida la emisión acelerada y la ejecución de una orden de suministrar información o de una orden de registro y confiscación de los datos. El principal requisito es contar con un proceso sumamente rápido para evitar que los datos se pierdan irreparablemente.
284. El párrafo 2 establece el contenido de una solicitud de conservación con arreglo a lo dispuesto en este artículo. Teniendo en cuenta que se trata de una medida provisional y que la petición tendrá que ser preparada y transmitida rápidamente, la información suministrada será sumaria e incluirá sólo la

información mínima necesaria para permitir la conservación de los datos. Además de especificar la autoridad que solicita la conservación y el delito por el cual se solicita la medida, la solicitud debe incluir una síntesis de los hechos, información suficiente para identificar los datos que han de preservarse y su ubicación, y demostrar que los datos son pertinentes para la investigación o el juicio relacionado con el delito en cuestión y que dicha conservación es necesaria. Por último, la Parte requirente debe comprometerse a presentar posteriormente una solicitud de asistencia mutua para poder obtener la presentación de los datos.

285. El párrafo 3 establece el principio de que no se exigirá como condición la doble tipificación penal para la conservación de los datos. En general, la aplicación del principio de doble tipificación penal es contraproducente en el contexto de la conservación de los datos. En primer lugar, como una cuestión de la práctica moderna respecto de la asistencia mutua, existe la tendencia a eliminar el requisito de la doble tipificación penal para todas las medidas procesales excepto las más intrusivas, tales como el registro y confiscación y la interceptación. Sin embargo, tal como fue prevista por quienes redactaron el Convenio, la conservación no es particularmente intrusiva, ya que el custodio simplemente conserva la posesión de los datos que están legalmente en su poder, y los datos no son revelados o examinados por funcionarios de la Parte requerida hasta después de la ejecución de una solicitud formal de asistencia mutua en que se solicite la divulgación de los datos. En segundo lugar, como cuestión práctica, a menudo lleva mucho tiempo proporcionar las aclaraciones necesarias para establecer de manera concluyente la existencia de la doble tipificación penal, y los datos podrían ser borrados, eliminados o alterados en el ínterin. Por ejemplo, en las primeras etapas de una investigación, la Parte requirente puede tener conocimiento de que se produjo una intrusión en un ordenador ubicado en su territorio, pero puede no comprender bien hasta mucho más tarde la naturaleza y magnitud del daño. Si la Parte requerida se demora en la conservación de los datos relativos al tráfico que pudieran servir para llegar hasta el origen de la intrusión, respecto de la cual está pendiente determinar la doble tipificación penal, los datos esenciales a menudo podrían ser eliminados de manera habitual por los proveedores de servicios que solo los conservan algunas horas o días después de efectuada la transmisión. Incluso si posteriormente la Parte requirente pudiera establecer la doble tipificación penal, los datos cruciales relativos al tráfico podrían no ser recuperados y el autor del delito nunca sería identificado.

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

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

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

demora, de modo que pueda evaluar si corre el riesgo planteado y sigue adelante con la solicitud de conservación, o si busca una manera más intrusiva, pero más segura, de procurar la asistencia mutua, como el procedimiento de registro y confiscación.

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

30 Artículo 30 – Revelación rápida de datos conservados

30.1 Disposiciones de la Convención

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.
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.

30.2 Examples

PORTUGAL
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 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.

ROMANIA, ART.64 of Romania Law no 161/2003

Art.64 - If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.

GERMANY
Article 30 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("**IRG**") in the absence of applicable international agreements, see Article 25 above.

30.3 Informe explicativo

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

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

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

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

31.1 Disposiciones de la Convención

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 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.

31.2 Examples

PORTUGAL
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 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.

ROMANIA, ART. 60 of Romania Law no 161/2003

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.
(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

GERMANY
Article 31 is covered by Sections 66 and 67 of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("**IRG**") in the absence of applicable international agreements, see Article 29 above.

24.3 Informe explicativo

Asistencia mutua en relación con el acceso a datos almacenados (Artículo 31)
292. Cada Parte debe tener, para beneficio de la otra Parte, la capacidad de registrar, o acceder de manera similar, y de confiscar, o conseguir de manera similar, y de revelar los datos almacenados por medio de un sistema informático situado en su territorio -- al igual que en virtud del Artículo 19 (Registro y confiscación de datos informáticos almacenados) debe tener la capacidad de hacerlo a nivel nacional. El párrafo 1 autoriza a una Parte a requerir este tipo de asistencia mutua, y el párrafo 2 establece que la Parte requerida debe poder proporcionarla. El párrafo 2 sigue también el principio de que los términos y condiciones para proveer dicha cooperación deberían ser los establecidos en los tratados aplicables, los acuerdos y las leyes nacionales que rigen la asistencia jurídica mutua en materia penal. En virtud del párrafo 3, deberá darse respuesta a dicha solicitud de forma acelerada cuando (1) existen motivos para creer que los datos pertinentes son particularmente vulnerables a sufrir pérdida o modificación, o (2) cuando esos tratados, acuerdos o leyes así lo establezcan.

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

32.1 Disposiciones de la Convención

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
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

32.2 Examples

PORTUGAL
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.

ROMANIA, ART.65 of Romania Law no 161/2003
Art.65 - (1) A competent foreign authority can have access to public Romanian sources of computer data without requesting the Romanian authorities.
(2) A competent foreign authority can have access and can receive, by means of a computer system located on its territory, computer data stored in Romania, if it has the approval of the authorised person, under the conditions of the law, to make them available by means of that computer system, without requesting the Romanian authorities.

GERMANY - German Code of Criminal Procedure (Strafprozessordnung), 2008 ("**StPO**"):
Section 94 - Objects Which May Be Seized
(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

32.3 Informe explicativo

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

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

294. El Artículo 32 (Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público) aborda dos situaciones: primero, cuando los datos a los que se ha de acceder sean accesibles al público y segundo, cuando una Parte ha accedido a datos o recibido datos ubicados fuera de su territorio a través de un sistema informático de su territorio y ha obtenido el consentimiento legal y voluntario de la persona que tiene autoridad legal para revelar los datos a la Parte a través de ese sistema. La cuestión de quién está "legítimamente autorizado" a revelar datos puede variar dependiendo de las circunstancias, la naturaleza de la persona y la ley aplicable de que se trate. Por ejemplo, el correo electrónico de una persona puede estar almacenado en otro país por un proveedor de servicios, o una persona puede deliberadamente almacenar datos en otro país. Estas personas pueden recuperar los datos y, siempre que tengan la autoridad legal, pueden voluntariamente revelar los datos a los agentes del orden o permitir a esos funcionarios acceder a los datos, según lo dispuesto en el artículo.

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

33.1 Disposiciones de la Convención

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.

33.2 Examples

PORTUGAL
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.

ROMANIA, ART. 60 of Romania Law no 161/2003

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.
(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

GERMANY
Article 33 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("**IRG**") in the absence of applicable international agreements, see Article 25 above.

33.3 Informe explicativo

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

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

296. En muchos países, la asistencia mutua se proporciona ampliamente respecto de la obtención en tiempo real de datos relativos al tráfico, porque dicha obtención de datos es considerada menos intrusiva que la interceptación de datos relativos al contenido o el registro y la confiscación. Sin embargo, una serie de Estados han adoptado un enfoque más restringido. En consecuencia, de la misma manera que las Partes pueden formular una reserva conforme al Artículo 14 (Ámbito de aplicación de las disposiciones de procedimiento), párrafo 3, con respecto al alcance de la medida equivalente a nivel nacional, el párrafo 2 permite a las Partes limitar el ámbito de aplicación de esta medida a una serie más restringida de delitos que los establecidos en el Artículo 23 (Principios generales relativos a la cooperación internacional). Se formula una advertencia: en ningún caso la serie de delitos puede ser más limitada que la serie de delitos para la cual tal medida está disponible en un caso equivalente a nivel nacional. En efecto, debido a que la obtención en tiempo real del los datos relativos al tráfico es a veces la única manera de determinar la identidad del autor de un delito, y debido al carácter menos intrusivo de la medida, el uso de la expresión "al menos" en el párrafo 2 se ha concebido para alentar a las Partes a permitir la asistencia más amplia posible, es decir, incluso en ausencia de doble tipificación penal.

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

34.1 Disposiciones de la Convención

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

34.2 Examples

PORTUGAL
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.

ROMANIA, ART. 60 of Romania Law no 161/2003

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.
(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

GERMANY

Article 34 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("**IRG**") in the absence of applicable international agreements, see Article 25 above

34.3 Informe explicativo

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

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