EL PAcCTO
EUROPA ↔ LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

LEY MODELO DE PRUEBA ELECTRÓNICA

Claudia Criscioni

Pedro Verdelho

Francisco Hernández Guerrero

Ediciones EL PAcCTO
Colección Herramientas

LEY MODELO DE PRUEBA ELECTRÓNICA

Claudia Criscioni

Pedro Verdelho

Francisco Hernández Guerrero

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Edita: Programa EL PAcCTO
Calle Almansa 105
28040 Madrid (España)
www.elpaccto.eu

Bajo la coordinación de:

FIIAPP

EXPERTISE FRANCE

Edición no venal

Esta publicación ha sido elaborada con la financiación de la Unión Europea. Su contenido es solo responsabilidad del programa "EL PAcCTO" y no refleja necesariamente las opiniones de la Unión Europea.

Prólogo

La lucha contra la delincuencia organizada requiere cada vez más una actuación especializada que nunca puede ser prevista a través de sistemas formativos tradicionales. Por el contrario, la nueva delincuencia no conoce fronteras y tiene a su disposición medios tecnológicos que le permiten cometer delitos o disfrutar de sus productos en otros estados y disposición de personal muy especializado que le permite la constitución de entramados societarios y contables de muy difícil verificación. En la actualidad, la tecnología cubre todos los ámbitos y es habitual el uso de medios de esta naturaleza para cualquier actuación por parte de todas las personas, lógicamente, también los delincuentes.
Puede definirse como prueba electrónica toda información con valor probatorio contenida en un medio electrónico o transmitida por dicho medio. Tal y como se definen, son precisos algunos presupuestos de validez:

- *La prueba electrónica se debe obtener de manera lícita.*
- *Deben respetarse los derechos fundamentales.*
- *Debe respetarse la cadena de custodia de la prueba digital y evitar manipulaciones.*
- *Debe acreditarse la autenticidad e integridad del material.*
- *Puede requerir el acompañamiento de un informe pericial técnico.*

Cada vez más, es preciso el análisis de los medios tecnológicos en las investigaciones penales: correos electrónicos, registro de transferencias y operaciones bancarias, incorporación de material videográfico, registro de asignación de IP, análisis remotos de ordenadores, terminales telefónicos y otros instrumentos, apertura de “cajas negras” en determinados accidentes, etc. Y no se trata de investigar únicamente el cibercrimen o el lavado de activos: todos los delitos (desde los más comunes a los más complejos) pueden requerir la prueba electrónica.

Durante el año 2021, EL PAcCTO desarrolló un análisis de la legislación en los estados, observándose que la mayoría de los Códigos Procesales Penales, aun con sus diferencias de matices, cuentan con una matriz o estructura de proceso penal común influida por la tradición jurídica europeo continental y marcada por el movimiento de reforma hacia los sistemas acusatorios dejando de lado los viejos modelos inquisitivos. Esta similitud de los sistemas es una gran ventaja que permite trabajar en líneas básicas de reformas procesales que sirvan de base para la adecuación de los códigos, tomando el set de medidas procesales básicas de la Convención de Budapest (y su futuro Segundo Protocolo Adicional) e incorporando medios de investigación en entornos digitales tales como el agente encubierto digital, entregas vigiladas en entornos digitales, drones, o las técnicas de remote forensic, de acuerdo con las decisiones políticas en cada uno de los países. Este manual actuaría como una guía de redacción de normas en la que deberían también tomarse en consideración las buenas prácticas del derecho comparado, la jurisprudencia sobre la materia más relevante de los órganos nacionales e internacionales y las recomendaciones de los organismos de derechos humanos. Este análisis fue realizado por los señores Sixto Luque Delgado, Marcos Salt, Carlos Pinho y Pedro Verdelho, con el título La prueba electrónica en el marco nacional e internacional en Latinoamérica (https://www.elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf).

En este panorama, el Ciclo Político de justicia compartida entre la Unión Europea y Latinoamérica, conformado en junio de 2022 por la Asociación Iberoamericana de Ministerios Públicos, la Conferencia de Ministros y Ministras de Justicia de los Países Iberoamericanos y la Cumbre Judicial

Iberoamericana acordó el desarrollo de una política común entre las organizaciones para fomentar la mejora normativa y la práctica de los estados en este precisa dirección. Con este propósito nace este texto.

La génesis de este texto merece ser explicada. Surgida como una formulación abstracta con origen en el estudio realizado y publicado en 2021, devino rápidamente concreta al producirse el feliz encuentro con el proyecto que estaba orientando la Corte Suprema de Justicia de Paraguay. Tras un conjunto de reuniones virtuales entre los expertos del programa y las altas personalidades designadas por el poder judicial de Paraguay, se puede redactar un texto adaptado. Esto es, si la idea original era formular un texto abstracto susceptible de adaptación posterior a cada nación, en este caso el proyecto nacional sirve de base para este texto más abstracto, de ahí su alto interés.
La señora Claudia Criscioni firma la introducción, pero su labor y participación orientó enormemente el texto elaborado por los señores Pedro Verdelho y Francisco Hernández Guerrero.

Antonio Roma Valdés

Introducción Por Claudia Criscionio

Es para mí un honor que me hayan solicitado hacer una introducción sobre el trabajo realizado por los expertos del programa EL PACTO respecto a una ley modelo de prueba electrónica para Latinoamérica.

La prueba digital resulta indispensable para una persecución penal eficiente y su adecuada regulación es también indispensable en el marco de un proceso penal respetuoso de las garantías constitucionales establecidas en un Estado de derecho.

Con relación al Paraguay, precisamente hemos solicitado la cooperación de los expertos a fin de elaborar un proyecto de ley de prueba electrónica para el proceso penal que finalmente fue presentado a la Comisión de Reforma del Código penal y procesal penal paraguayo.

El punto de partida ha sido la necesidad de contar con una normativa que regule estos medios de prueba, así como su obtención y producción.

El Paraguay al igual que la mayoría de los países de la región aprobó la "Convención sobre la Ciberdelincuencia" adoptado por el Consejo de Europa en la 109ª Reunión del Comité de Ministros del Consejo de Europa, el 23 de noviembre de 2001, y el "Protocolo Adicional al Convenio sobre Ciberdelincuencia Relativo a la Penalización de Actos de índole Racista y Xenófoba cometidos por medio de Sistemas Informáticos", adoptada en la ciudad de Estrasburgo, el 28 de enero de 2003 y en consecuencia mediante una modificación al Código Penal, estableció los hechos punibles adecuando su regulación a las previsiones del Convenio de Budapest, sin embargo, el derecho procesal penal constituye una materia pendiente y en consecuencia la cooperación internacional se ve afectada ante la falta de regulación.

Es por ello, que conscientes del desafío que representa, tanto a nivel teórico como práctico, la regulación de formas de investigación y medios de prueba para asegurar la recolección y preservación de la evidencia digital, garantizando su autenticidad e integridad y desechada la idea de que el principio de libertad probatoria permite la incorporación de cualquier medio de prueba al proceso penal, hemos querido adoptar una ley que regule de manera precisa los principios rectores en la materia.

No hago una exposición novedosa afirmando que todo lo relacionado a la prueba digital supera las previsiones legales en torno a la evidencia física, pero lo que sí puedo afirmar es que para su regulación es indispensable tener en cuenta la experiencia de operadores de justicia cuyos ordenamientos jurídicos ya cuentan con legislación y jurisprudencia afianzada en la materia.

Es por eso que tal y como se describe en este trabajo realizado por los expertos, hemos obtenido "los insumos" y hemos preparado un proyecto de ley orientado en las normas de cooperación internacional y las normas procesales, no solo del Convenido de Budapest y su primer protocolo, sino que también del segundo protocolo, por lo que se constituye en un proyecto de ley bastante actualizado en lo que hace a la previsión de medios de prueba electrónica.

Para el Paraguay, hemos optado por proponer la inclusión de un título dentro de los medios de prueba en el Código procesal penal, que regule los medios de prueba electrónica.

Consultado con el parecer de los expertos, la inclusión en el Código procesal penal de los medios de prueba electrónicos, garantiza que los aplicadores del derecho sean más reflexivos respecto a sus presupuestos que si se los regula en una ley especial.

Es por ello que, siguiendo la reforma procesal española, adaptando algunos preceptos al proceso penal paraguayo, orientado en el Código procesal penal tipo para Latinoamérica, hemos redactado un proyecto de ley que tiene las siguientes características:

En el entendimiento que la regulación debía cumplir con estándares que permitan la cooperación internacional, en el entendimiento que la investigación y persecución efectiva de hechos punibles supera el ámbito de aplicación de un territorio, lo que torna necesario el acceso a medios de prueba obtenidos fuera del territorio nacional que puedan ser incorporados al proceso penal, hemos orientamos la normativa en los principios de especialidad y proporcionalidad.

En cuanto al ámbito de aplicación, vale decir en qué casos podrán ser utilizados estos medios prueba, en estricto cumplimiento al principio de especialidad, hemos establecido un catálogo muy preciso de los hechos punibles que podrían ser investigados.

En cuanto al principio de proporcionalidad, a fin de hacerlo operativo, hemos incorporado una definición de este principio que debe ser atendido por los operadores de justicia.

También hemos tenido especial cuidado en los plazos de duración de las medidas conforme a su intensidad en la intromisión a los derechos fundamentales del imputado por lo que establecido plazo para cada medida.

En este punto, la intervención de los expertos ha sido de fundamental importancia, puesto que con su experiencia nos han podido orientar respecto al establecimiento de plazos que a su vez son necesarios para la efectividad de la medida.

Igualmente, a fin de que la ley garantice efectivamente el respecto a los principios rectores, se describen acabadamente los presupuestos para la solicitud de una autorización judicial, así como el contenido de la resolución judicial que autoriza una medida de investigación tecnológica.

Se previó además el control de las medidas y las condiciones para la destrucción de los registros originales que consten en sistemas electrónicos o informáticos utilizados en la ejecución de las medidas.

Asimismo, a falta de una regulación general en el Código procesal penal paraguayo, se incluyó un artículo que regula la utilización de la información obtenida en otro proceso y los hallazgos inevitables.

Concretamente hemos regulado las siguientes medidas:

- *El Aseguramiento de datos. La Orden de presentación.*

- *El Acceso transfronterizo a datos informáticos, de acceso público o con consentimiento.*

- *La Interceptación de comunicaciones telefónicas y telemáticas. En esta medida en particular debe destacarse el aporte invaluable de los expertos en la regulación respecto al acceso de las partes a las grabaciones.*

- *La incorporación al proceso de datos electrónicos de tráfico o asociados. Datos obrantes en archivos automatizados de los prestadores de servicio y búsqueda entrecruzada o inteligente de datos.*

- *El acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad. La Identificación mediante número IP.*

- *La identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.*

- *La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos: la grabación de las comunicaciones orales directas y obtención de imágenes.*

- *La utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. La captación de imágenes en lugares o espacios públicos.*

- *La utilización de dispositivos o medios técnicos de seguimiento y localización.*

- *El registro de dispositivos de almacenamiento masivo de información.*

- *El registro y secuestro de datos.*

- *El acceso a la información de dispositivos electrónicos incautados en lugares públicos.*

- *El registro remoto sobre equipos informáticos.*

- *Y por último: el agente encubierto digital.*

De ser aprobado el proyecto de ley, sería una herramienta fundamental para el Paraguay, sin lugar a dudas esto no hubiera sido posible sin el apoyo de los expertos que nos han brindado su conocimiento y experiencia, por lo que va para ellos mi más sincero agradecimiento.

Ley Modelo de prueba electrónica

La necesidad de una Ley modelo de prueba electrónica

La constitución en Bruselas en junio de 2022 del llamado Ciclo Político de Justicia por el acuerdo de las grandes entidades birregionales de justicia, la Asociación Iberoamericana de Ministerios Públicos (AIAMP), la Conferencia de Ministros y Ministras de Justicia de los Países Iberoamericanos (COMJIB) y la Cumbre Judicial Iberoamericana supone un gran paso adelante en la definición de políticas públicas de justicia penal basada en valores comunes a ambos lados del Océano Atlántico.

El apartado 5 letra c) de la Declaración de Bruselas propugna entre sus objetivos la generalización del uso de medios de prueba electrónica en los procesos penales, con atención a su obtención, custodia e interpretación, también en línea con lo dispuesto en el Convenio de Budapest y en el Segundo Protocolo, relativo a la obtención de pruebas electrónicas en las investigaciones y procesos penales que involucran a más de un estado.

El Programa EPAcCTO desarrolló una actividad en 2021 que dio ocasión a la publicación de un análisis relevante: La prueba electrónica en el marco nacional y en el internacional en Latinoamérica, redactado por Sixto Luque Delgado, Marcos Salt, Carlos Pinho y Pedro Verdelho, que se publicó el 14 de febrero de 2022.

Se pretendió estudiar en concreto la forma de obtener prueba electrónica en investigaciones criminales, con miras a dibujar una ley modelo de evidencia digital para el marco jurídico y el contexto latino americano. La legislación nacional no puede quedar al margen de esta evolución. Es preciso que los operadores nacionales cuenten con armas legales suficientes para solicitar la asistencia y evitar la impunidad de las formas más graves de delincuencia. El presente articulado responde a esta necesidad.

Sobre esta necesidad y los antecedentes mencionados, esta ley se propone contribuir a los objetivos del Ciclo Político de Justicia compartido entre la Unión Europea y América Latina.

Metodología de trabajo

Como método de trabajo, se decidió, en un primer momento, definir las grandes líneas que, en concreto, deberían incorporarse en una ley modelo de prueba electrónica para Latinoamérica.

Se tuvo como referencia primera y como fuente de inspiración, la parte procesal del Convenio de Budapest. Este tratado internacional, reconocidamente el gran marco (y, además, único, por el momento) a nivel global sobre ciberdelito y evidencias digitales, fue ya ratificado por muchos de los países de Latinoamérica. Incluye normas de derecho penal sustantivo, normas de cooperación internacional y también normas procesales.

Estas últimas se describen en los artículos 14 a 21 del convenio. En la elaboración de este borrador de ley modelo de prueba electrónica se dio particular enfoque a los artículos 16, 17, 18 y también 32 del Convenio de Budapest que, si bien, no es parte integrante del apartado de derecho penal sustantivo, incluye normas procesales y con repercusión procesal.

Se tomó también como fuente de inspiración el Segundo Protocolo Adicional al Convenio de Budapest. Se trata de un nuevo tratado internacional, abierto a firma a 12 de mayo de 2022 y todavía no en vigor, aunque lo tengan firmado ya más de 30 Estados Parte del Convenio de Budapest. Este Segundo Protocolo incluye muchas y muy interesantes normas procesales, algunas de ellas muy originales, sobre todo en la arena internacional.

Como ejercicio paralelo y concreto, se partió para la discusión de un borrador específico, que pudiera ser aplicable a un concreto país. Con inspiración en el modelo genérico, redactado por expertos de ELPAcCTO, personas expertas designadas por la Corte Suprema de Justicia de Paraguay redactaron un concreto borrador de proyecto de ley que, modificando al Código Procesal Penal, introdujera normas de obtención de prueba digital.

Las fuentes de inspiración han sido las mismas, ya que Paraguay es un Estado Parte del Convenio de Budapest.

Sin embargo, en este caso, se recurrió también a la reforma procesal penal española del año 2015 que introdujo modernas formas de recoger pruebas electrónicas – y, además, al tener el sistema jurídico paraguayo gran comunidad de principios con el sistema español.

En este ejercicio concreto se determinaron los principios generales y régimen común de las diligencias tecnológicas (autoridad habilitante, solicitudes, resoluciones habilitantes, plazos y prórrogas, causas de cese, garantías tecnológicas, afectación a terceros, empleo en otros procedimientos, hallazgos causales y ampliaciones, conservación, cancelación y supresión de soportes y registros).

Después, se seleccionaron las medidas concretas a incorporar en el Código Procesal. Se concretaron los regímenes jurídicos de cada una, conforme a los patrones de referencia. Después de una primera redacción, el grupo de trabajo que se constituyó en Paraguay discutió el borrador, con los expertos de ELPAcCTO y se llegó a una versión final. Dicha versión se presentó a representantes del poder legislativo de Paraguay.

Después, se celebró otra reunión en este ámbito, el día 5 de julio de 2022. Esta reunión, también de modo totalmente virtual, tenía el propósito de facilitar la discusión del tema con representantes de la CJI – Cumbre Judicial de Iberoamérica (en su representación fueron invitados Juan Martínez, Luis de Arcos Pérez, Sandra Zúñiga Morales y otros representantes del Poder Judicial de Costa Rica), representantes de la COMJIB – Conferencia de Ministros de Justicia de Iberoamérica (en su representación fueron invitados Tatiana Salem y Javier Samper Orgilés) y representantes de dos de las Redes de la AIAMP – Asociación Ibero-Americana de Ministerios Públicos (la RedCoop, representada por Antonio Segovia y CiberRed).

La primera reunión específica con las autoridades de Paraguay se celebró el día 7 de abril de 2022. Después de ella se celebraron otras (los días 18 de abril, 20 de mayo, 17 de junio, 12 de julio y 4 de octubre). En ellas participaron distintos representantes de las autoridades del Poder Judicial de Paraguay: los ministros profesores doctores Luis María Benítez Riera, Manuel Ramírez Candia, María Carolina Llanes, las magistradas Claudia Crisccioni, Yolanda Portillo y Yolanda Morel, así como la Abogada Mónica Paredes, Directora de Cooperación y Asistencia Judicial Internacional. Se celebró una sesión más, el día 10 de octubre de 2022, con el propósito de presentar este borrador a representantes del poder legislativo de Paraguay.

Con todo ello, se ha elaborado un texto polivalente susceptible de ser adaptado a cada ordenamiento jurídico, cuidando de los ajustes correspondientes. Es una apuesta de futuro para una necesidad bien actual.

Para el futuro quedan otras necesidades como las derivadas, por ejemplo, de la inteligencia artificial.

.Características

El texto de esta Ley Modelo puede incorporarse como ley especial de manera autónoma o bien ser introducido en el Código de Procedimiento Penal.

Debemos llamar la atención sobre un punto fundamental: el régimen de autorizaciones cambia de un estado a otro. Según las materias, algunas de las materias mencionadas en este texto pueden ser realizadas por jueces, por el ministerio público o por la policía, dependiendo de cada estado. Por esta razón, hemos optado por el empleo de una forma abstracta de remisión, normalmente la autoridad, advirtiendo en rojo este aspecto para que la adaptación a cada ordenamiento jurídico se realice de manera respetuosa con las características que le son propias.

No hemos referido determinados aspectos de la posible investigación digital tales como:

a) Captación de emisiones térmicas en el interior de edificios, domicilios y lugares cerrados.

b) Investigaciones y seguimientos físicos sistemáticos.

c) Medios de investigación basados en datos protegidos recabados de forma sistemática.

d) Autorizaciones de las medidas de investigación tecnológica en casos de urgencia, con posterior ratificación.

Capítulo I
Disposiciones comunes a las medidas de investigación tecnológicas

Artículo 1. Ámbito de aplicación de esta ley

1. Los poderes y procedimientos previstos en esta ley podrán aplicarse cuando sean precisos para el esclarecimiento de un delito concreto, para la determinación de sus responsables, para su localización y la de los efectos o instrumentos de comisión de los hechos investigados.

2. Los poderes y procedimientos previstos en esta Ley se aplicarán a las investigaciones:

a) Por delitos castigados con pena cuyo límite máximo sea igual o superior a dos años de prisión. No obstante, determinadas medidas solo podrán adoptarse en los casos expresamente previstos.

b) Por delitos cometidos a través de dispositivos o servicios informáticos o de comunicaciones, o de cualquier servicio o tecnología de la información o de las comunicaciones.

c) Para la obtención de pruebas electrónicas de un delito, si los datos o documentos necesarios para su acreditación se encuentran exclusivamente en esta forma.

Artículo 2. Condiciones y salvaguardias

1. La aplicación y ejecución de las normas procesales previstas en la presente ley estarán sujetas a las condiciones y salvaguardas generales previstas en el derecho procesal penal interno.

2. Deberá garantizarse una protección adecuada de los derechos humanos y de las libertades públicas, incluidos los derechos derivados de los tratados internacionales para la protección de los derechos humanos y las libertades fundamentales, derechos civiles y políticos, así como de las leyes sectoriales de aplicación.

3. Las condiciones de aplicación de esta ley incluyen, siempre que resulte procedente de la naturaleza del procedimiento, la intervención o supervisión, la motivación de la solicitud de adoptación y de la resolución autorizante, la limitación del ámbito de aplicación y de la duración del procedimiento.

4. Las salvaguardas y garantías se extenderán al resultado de las medidas de investigación desarrolladas, una vez concluido, así como a su posible empleo en otros procedimientos.

Artículo 3. Principios de aplicación

1. La adopción de las medidas de investigación previstas en este título se someterá plenamente a los principios de especialidad, idoneidad, necesidad y proporcionalidad.

2. Las medidas previstas en este título solo podrán acordarse en la investigación de un delito concreto, siempre que exista una evidencia o indicio objetivo que la justifique. En ningún caso podrán tener como finalidad la prevención de la comisión de hechos futuros.

3. Las medidas de investigación tecnológica tendrán que ser útiles para la averiguación de los hechos, de sus responsables y de sus efectos o instrumentos.

4. Los poderes de investigación tecnológicos solo podrán emplearse cuando no haya medidas menos gravosas para los derechos fundamentales y procesales del investigado e igualmente útiles para los fines de la investigación.
Para determinar la gravosidad de la medida se tendrán en cuenta los medios a disposición de las autoridades y de los agentes encargados de su investigación, y el perjuicio que pueda depararse al proceso de no emplearse.

5. Las medidas de investigación contempladas en este título se considerarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Artículo 4. 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 esta 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) «servicio de comunicaciones interpersonales»: el prestado por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio.

Artículo 5. Contenido de la resolución autorizante

1. La autorización de la medida se resolverá mediante resolución motivada.

2. La resolución que autorice la medida concretará al menos los siguientes extremos:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 3.

d) La duración de la medida.

e) La finalidad perseguida con la medida.

Artículo 6. Duración de las medidas

1. Las medidas tendrán la duración que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.

2. La medida podrá ser prorrogada, mediante resolución motivada, siempre que subsistan las causas que la motivaron.

3. Se acordará el cese de la medida cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos, y, en todo caso, cuando haya transcurrido el plazo para el que hubiera sido acordada.

Artículo 7. Medidas de custodia de las pruebas electrónicas obtenidas

1. Las grabaciones de imágenes, sonidos, datos de tráfico y de localización, señales y emisiones de todo tipo, así como los datos e informaciones obtenidos por medio de las diligencias de investigación, se conservarán por las autoridades que las hayan recabado o recibido, de modo que se garantice su confidencialidad y restricción de uso al procedimiento en que fueron autorizadas.

2. Las pruebas electrónicas obtenidas serán sometidas a las medidas técnicas y organizativas precisas para garantizar su autenticidad e integridad, tanto durante el proceso de obtención y tratamiento como el posterior de custodia y archivo.

3. Si fuere preciso el tratamiento informático de su contenido para facilitar su interpretación, visualización o audición, se preservará en todo caso la evidencia original de la que se realizará una copia para su tratamiento técnico a esos fines.

4. La autoridad que las acuerde adoptará las medidas técnicas adecuadas para posibilitar la realización de un dictamen pericial sobre las pruebas obtenidas.
La autorización para la elaboración de un dictamen pericial para acreditar la autenticidad o integridad de la prueba obtenida, o el correcto funcionamiento de los medios físicos o lógicos empleados para obtenerlas, requerirá la acreditación de un indicio fundado de alteración, manipulación o mal funcionamiento, en su caso.

5. Las comunicaciones con los sujetos obligados a prestar colaboración podrán realizarse en formato electrónico, siempre que sean autenticadas con los mecanismos de firma electrónica avanzada a disposición de las autoridades intervinientes.

6. Para la adopción y ejecución de las medidas mencionadas en este artículo se tendrá en cuenta el estado de la tecnología al tiempo de su adopción o ejecución, y especialmente los estándares sectoriales internacionales vigentes.

Artículo 8. Utilización de la información obtenida en otros procedimientos y hallazgos casuales

1. Los elementos de convicción obtenidos como resultado de las medidas previstas en este capítulo podrán ser utilizados en otro proceso penal. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia, que contendrá en todo caso los antecedentes indispensables, la solicitud inicial de adopción, y la resolución que la hubiere acordado o prorrogado.

2. La continuación de una de las medidas previstas en este título para la investigación del delito casualmente descubierto requerirá de autorización de la autoridad. Para ello, se comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento.

Artículo 9. Afectación de terceras personas

Podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

Artículo 10. Deber de colaboración

1. Todos los prestadores de servicios de comunicaciones electrónicas, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información; titulares o responsables de sistemas informáticos de cualquier tipo, así como de bases de datos o registros de cualquier tipo; suministradores de servicios digitales de ciberseguridad o de mantenimiento o gestión de los equipos físicos o virtuales y bases de datos objeto de investigación, así como de así como toda persona que de cualquier modo contribuya a facilitar la comunicación investigada o la ejecución de la medida tecnológica de investigación, están obligados a prestar la asistencia y colaboración precisas para facilitar el cumplimiento de las resoluciones de adopción.

2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en responsabilidad penal.

Artículo 11. Conservación y destrucción de la información y registros obtenidos

1. Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia de la autoridad.

2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio de la corte.

Capítulo II
Aseguramiento y acceso a datos e información

Sección Primera
Aseguramiento de datos

Artículo 12. Aseguramiento de datos

1. Por decisión del Ministerio Público se podrá ordenar a cualquier persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema informático que esté a su disposición y control cuando tenga motivos para sospechar que estos datos pueden ser alterados o suprimidos. La orden deberá especificar los datos concretos que pretende asegurar. La medida no podrá exceder de noventa días, prorrogables por una sola vez si se mantienen los motivos que fundamentaron la orden.

2. La persona requerida deberá arbitrar los medios necesarios para preservar de inmediato los datos en cuestión, estando obligada a prestar su colaboración en la ejecución de la medida y a mantener secreto de su desarrollo bajo el apercibimiento de incurrir en delito.
3. En los casos de órdenes de aseguramiento de datos de tráfico de comunicaciones, cuando el proveedor de servicios requerido advierta que en la comunicación que es objeto de investigación hayan participado otros proveedores de servicios, lo informará a la autoridad que emitió la orden a fin de que adopte las medidas de aseguramiento necesarias en relación con ellos.

Sección Segunda
Acceso a datos

Artículo 13. Órdenes de presentación

1. El Ministerio Público podrá ordenar a cualquier persona física o jurídica, que presente, remita, entregue o ponga a su disposición datos alojados en un sistema informático que esté bajo su poder o control y que se vinculen con la investigación de un delito concreto.

2. Asimismo, el Ministerio Público podrá ordenar a toda persona física o jurídica que preste un servicio de comunicaciones o a los proveedores de servicios de internet de cualquier tipo, la entrega de datos de los usuarios o abonados o los datos de identificación y facturación con los que cuente. La orden contendrá la indicación de que la medida deberá mantenerse en secreto bajo el apercibimiento de sanción penal.

3. De acuerdo con los acuerdos internacionales establecidos, se podrá ordenar a cualquier persona física o jurídica, que preste servicios de registro de nombres de dominio que presente, remita o entregue información en su poder o esté bajo su control, con el fin de hallar al registrante de un nombre de dominio o ponerse en contacto con él.

La solicitud a que se refiere este apartado incluirá:

> *a) la fecha de expedición, así como la identidad y los datos de contacto de la autoridad competente que haya cursado la solicitud;*

b) el nombre de dominio sobre el que se solicita información y una lista pormenorizada de la información que se pide, con desglose de los elementos de datos concretos;

c) una declaración de que la solicitud se refiere a información pertinente para una investigación o proceso penal específico y de que la información solo se utilizará para esa investigación o proceso penal específico;

d) el plazo y la forma en que se deberá revelar la información, y cualesquiera otras instrucciones procesales especiales.

Si la entidad lo aceptara, se podrá presentar la solicitud en formato electrónico.

3. De acuerdo con los acuerdos internacionales establecidos, el Ministerio Público podrá ordenar a un proveedor de servicios, con el fin de obtener información almacenada relativa a abonados específica que obre en poder o esté bajo el control de dicho proveedor de servicios, cuando la información relativa a abonados sea necesaria para las investigaciones o procesos penales específicos.

La orden mencionada especificará:

a) la autoridad expedidora y la fecha de expedición;

b) el nombre y la dirección del proveedor o proveedores de servicios a los que se debe dar traslado del requerimiento;

c) el delito o delitos que son objeto de la investigación o proceso penal;

d) la autoridad que necesita la información específica relativa a abonados cuando no sea la autoridad emisora; y

e) una descripción pormenorizada de la información específica relativa a abonados que se pide.

El requerimiento contemplado en este apartado irá acompañado de la información suplementaria siguiente:

a) los fundamentos jurídicos nacionales que facultan a la autoridad para dictar el orden;

b) una referencia a las disposiciones legales y sanciones aplicables al delito investigado o enjuiciado;

c) la información de contacto de la autoridad a la que el proveedor de servicios enviará la información relativa a abonados, a la que podrá solicitar más información o a la que deberá responder de algún otro modo;

d) el plazo y la forma en que se deberá enviar la información relativa a abonados;

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

f) cualesquiera instrucciones procesales especiales;

g) cualquier otra información que pueda ayudar a obtener la revelación de la información relativa a abonados.

Artículo 14. Acceso transfronterizo a datos informáticos, de acceso público o con consentimiento

1. De conformidad con lo dispuesto en tratados y convenciones internacionales, las autoridades nacionales podrán acceder, sin necesidad de autorización, a datos informáticos almacenados en un sistema informático ubicado en otro Estado cuando estos estén a disposición del público; o recibir o acceder, por medio de un sistema informático ubicado en el país a datos informáticos almacenados en otro Estado, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos.

2. Idéntico acceso es permitido a las autoridades extranjeras competentes, sin previa petición a las autoridades nacionales.

Capítulo III
Interceptación de comunicaciones interpersonales y telemáticas

Sección Primera
Disposiciones generales

Artículo 15. Presupuestos de aplicación

1. La autoridad podrá ordenar por resolución fundada la interceptación de las comunicaciones interpersonales y telemáticas solo cuando la investigación tenga por objeto:

a) un hecho punible esté sancionado con pena privativa de libertad igual o superior a los tres años, o

b) un hecho punible cometido a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación, cualquiera que sea su límite punitivo.

2. La interceptación de las comunicaciones se podrá acordar cuando concurran los siguientes requisitos:

Que existan indicios, basados en datos objetivos, de la comisión de alguno de los delitos a que se refiere el apartado anterior.

b) Que sea previsible la obtención de datos relevantes para el descubrimiento o la comprobación del hecho investigado, para la determinación de su autor o para la averiguación de su paradero, siempre que tales informaciones no puedan obtenerse mediante otro medio de investigación menos gravoso.

c) Que exista una relación objetiva entre los hechos investigados y la línea telefónica o el medio o sistema de comunicación cuya intervención se pretende.

Artículo 16. Ámbito de la medida

1. Los terminales, físicos o virtuales, o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.

La intervención acordada podrá autorizar el acceso:

a) al simple conocimiento de su origen o destino

b) al contenido de las comunicaciones, o

c) a los datos electrónicos de tráfico o asociados al proceso de comunicación, o a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.

2. También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad por el delito investigado

3. Podrá acordarse la intervención de las comunicaciones emitidas desde terminales o medios telemáticos de comunicación pertenecientes a una tercera persona siempre que:

a) exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o

b) el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad, o

c) cuando el dispositivo o servicio objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

Artículo 17. Contenido de la resolución autorizante

La resolución que disponga la intervención de las comunicaciones concretará los siguientes extremos:

a) El hecho punible objeto de investigación y su calificación jurídica.

b) La identidad de los investigados y de cualquier otra persona afectada por la medida, de ser conocida.

c) El medio de telecomunicación objeto de la intervención, designando el número del teléfono intervenido o el código de identidad de las comunicaciones electrónicas, lógico o virtual, que sirva para identificar el medio de comunicación o telecomunicación de que se trate.

d) Los motivos por los cuales la diligencia resulta necesaria para el logro de los fines establecidos en esta ley.

e) La extensión de la medida especificando su alcance conforme a lo establecido en el artículo 15 de esta ley.

f) La forma de ejecución.

g) La duración de la medida.

h) Los sistemas y plazos de control

Artículo 18. Ampliación a nuevos hechos o personas

1. La autorización se entenderá únicamente concedida para la investigación del hecho delictivo que la motiva.

2. Si durante la ejecución de la diligencia aparecieran nuevos hechos punibles o se pudiera inferir la participación de otras personas, deberá resolverse la extensión a dichos hechos o personas la investigación por medio de la interceptación de comunicaciones interpersonales o telemáticas. Autorizada que fuera la intervención, sus efectos se extenderán a las comunicaciones ya obtenidas.

Artículo 19. Duración de la medida

1. La duración máxima inicial de la intervención, que se computará desde la fecha de la autorización, será de tres meses.
2. La interceptación podrá prorrogarse por períodos sucesivos de igual duración, hasta el plazo máximo de un año, si subsisten las causas que la motivaron.

Artículo 20. Control de la medida

En la resolución que autoriza la medida, la autoridad dispondrá la puesta a su disposición en soportes digitales distintos la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas cada treinta días. Se indicarán el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información obtenida desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.

Artículo 21. Acceso de las partes a las grabaciones

1. Expirada la vigencia de la medida de intervención, la autoridad entregará a las partes copia de las grabaciones íntegras y de las transcripciones realizadas. Si se advirtiera que en la grabación hubiera datos referidos a la vida íntima de las personas, se entregará la copia de la grabación y de la transcripción que no se refiera a ellas, lo que se hará constar de modo expreso.

De igual modo, podrá actuar el Ministerio Público en el caso de que las grabaciones contuvieran informaciones que pudiera afectar a futuras investigaciones. En ese caso, el Ministerio Público deberá motivar la solicitud de exclusión y presentar un principio de prueba que la acredite.

2. Examinadas las grabaciones y hasta la audiencia preliminar, el afectado podrá solicitar la inclusión en las copias de las grabaciones de aquellas comunicaciones concretas que considere relevantes y que hayan sido excluidas.

3. Se notificará a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia o del futuro.

4. La comparecencia mencionada se celebrará aunque alguna de las partes, debidamente notificadas, no compareciere a la misma.

Sección Segunda
Incorporación al proceso de datos electrónicos de tráfico o asociados

Artículo 22. Incorporación al proceso de datos electrónicos de tráfico o asociados

1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa, por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser entregados para su incorporación al proceso penal mediante orden de la autoridad.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se podrá recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser solicitados y los motivos que justifiquen la cesión.

Sección Tercera
Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

Artículo 23. Identificación mediante una dirección IP

Cuando en el ejercicio de las funciones de prevención e investigación se tuviera acceso a la dirección IP que estuviera siendo utilizada para la comisión de un hecho punible a través de internet, y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente, ni los datos de identificación personal del usuario, se podrá solicitar a los sujetos obligados en el artículo 10 la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospecho.

Artículo 24. Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes

Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, la autoridad podrá valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

Capítulo IV
Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Artículo 25. Captación y grabación de las comunicaciones orales directas

1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.

Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.

2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.

3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución que la acuerde.

Artículo 26. Presupuestos

1. La utilización de los dispositivos a que se refiere el artículo anterior ha de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación.

2. Solo podrá autorizarse cuando concurran los requisitos siguientes:

a) Que los hechos que estén siendo investigados sean constitutivos de alguno de los siguientes delitos:

1. Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2. Delitos cometidos en el seno de un grupo u organización criminal.

b) Que pueda racionalmente preverse que la utilización de los dispositivos aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor.

Artículo 27. Ámbito de la vigilancia acústica

1. Solo se podrá autorizar la escucha y grabación de las conversaciones privadas que mantenga la persona investigada. No obstante, también podrá practicarse esta medida de investigación aun cuando inevitablemente haya de verse afectada la intimidad de su interlocutor o de terceros.

2. La escucha y grabación no podrán extenderse a las conversaciones que la persona investigada mantenga con quienes estén dispensados de la obligación de declarar por razón de parentesco o de secreto profesional, salvo que el procedimiento también se dirija contra ellos.

3. Solo podrán captarse conversaciones que tengan lugar en el interior de un domicilio si es el de la persona investigada. Excepcionalmente, también se podrán captar las conversaciones que se mantengan en el domicilio de una tercera persona cuando existan indicios fundados de que la persona investigada se encuentre en él.

4. Queda prohibida la obtención de imágenes o sonidos en el interior del domicilio cuando afecte de forma directa y grave a la intimidad de los moradores.

Artículo 28. Contenido de la resolución habilitante

La resolución que autorice la medida, deberá contener, además de las exigencias reguladas en el artículo 5, una mención concreta al lugar o dependencias, así como a los encuentros del investigado que van a ser sometidos a vigilancia.

Artículo 29. Cese y ampliación de la medida

1. La escucha y grabación de las conversaciones privadas deberán ser dejadas sin efecto tan pronto dejen de existir los presupuestos que determinaron su adopción o se produzca el encuentro concreto para cuya grabación se autorizó.

2. Su ampliación para otros encuentros sucesivos habrá de ser objeto, cada uno de ellos, de una nueva autorización, que solo se podrá acordar cuando se den los mismos requisitos que motivaron su adopción.

Artículo 30. Comparecencia de la persona investigada

Concluida la intervención y documentadas las conversaciones en sus correspondientes soportes, la autoridad convocará a la persona investigada a una comparecencia para excluir aquellos extremos que no se encuentren relacionados con los hechos investigados o que, aun estándolo, sean irrelevantes para la investigación o cuya conservación no resulte necesaria para el ejercicio efectivo del derecho de defensa.

Capítulo V
Utilización de dispositivos técnicos de captación de la imagen, de seguimiento de localización

Artículo 31. Captación de imágenes en lugares o espacios públicos.

1. La autoridad podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuere necesario para facilitar su identificación, para localizar los instrumentos, objetos o productos del hecho punible u obtener datos relevantes para dilucidar los hechos investigados.

La captación simultánea de imagen y sonido, aun en lugares o espacios públicos, requerirá de autorización específica motivada.

2. La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación.

3. Para la captación y grabación de imágenes del interior de un domicilio o lugar cerrado que precise el empleo de medios técnicos para superar los obstáculos naturales o dispuestos por el titular o a su instancia, se requerirá autorización motivada en los términos previstos en el artículo

4. No podrán ser utilizadas las grabaciones obtenidas mediante dispositivos de grabación de la imagen por los servicios de vigilancia de instalaciones públicas y privadas cuando su instalación y uso no se encuentren autorizados conforme a la ley.

Artículo 32. Utilización de dispositivos o medios técnicos de seguimiento y localización.

1. Cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, la autoridad podrá acordar la utilización de dispositivos o medios técnicos de seguimiento y localización.

2. La autorización deberá especificar el medio técnico que va a ser utilizado

3. Con la finalidad de localizar en tiempo real a la persona investigada o conocer sus movimientos, se podrá autorizar que se recabe de los sujetos obligados mencionados en el artículo 10 la entrega de toda la información que posean sobre la situación geográfica o punto de terminación de red del origen y destino de las llamadas telefónicas realizadas o recibidas por la persona investigada.

Artículo 33. Duración de la medida

1. La medida de utilización de dispositivos técnicos de seguimiento y localización prevista en el artículo anterior tendrá una duración máxima de tres meses a partir de la fecha de su autorización. Excepcionalmente, podrán acordarse prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de dieciocho meses, si así estuviera justificado a la vista de los resultados obtenidos con la medida.

2. La información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida.

Capítulo VI
Registro de dispositivos de almacenamiento masivo de información

Sección Primera
Registro de dispositivos de almacenamiento de información

Artículo 34. Registro y secuestro de datos e información

1. La autoridad podrá ordenar el registro de un sistema informático, físico o virtual, o de una parte de este, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de:

a) secuestrar los componentes físicos y lógicos del sistema,

b) acceder a su contenido para su examen preliminar,

c) obtener copia de los datos en un soporte autónomo o

d) preservar por medios tecnológicos o bloquear el acceso a los datos de interés para la investigación.

2. Regirán en cuanto sean aplicables las normas generales y las mismas limitaciones dispuestas para el secuestro de documentos y correspondencia epistolar.

3. En los supuestos en los que, durante la ejecución de una medida de incautación de datos de un sistema Informático, previstos en el párrafo anterior, surjan indicios fundados que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático, físico o virtual, al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevaran adelante la medida podrán extenderla o ampliar el registro al otro sistema. La ampliación del registro a los fines de la incautación deberá ser autorizada por la autoridad salvo que estuviera prevista en la orden original.

Artículo 35. Necesidad de motivación individualizada

1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación interpersonal o telemática o dispositivos de almacenamiento masivo de información digital, físicos o virtuales, o el acceso a repositorios telemáticos de datos, la resolución de la autoridad habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. En los casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, físicos o virtuales, sean incautados en lugares públicos, se podrá autorizar el secuestro de tales efectos y el acceso a la información albergada en los dispositivos o accesible a través de ellos.

3. La simple incautación de cualquiera de los dispositivos a los que se refieren los apartados anteriores, practicada durante el transcurso de la diligencia de registro domiciliario o incautados en lugares o espacios públicos, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente.

4. La resolución que autorice el secuestro y acceso a los dispositivos físicos o virtuales objeto de investigación deberá precisar las medidas de acceso y examen de los dispositivos investigados, de obtención de copias de la información en ellos contenida, de preservación de los datos que no puedan ser recuperados o copiados durante el registro, de modo que no resulten afectadas la trazabilidad, autenticación e integridad de los datos e información recuperadas.

La autorización se extenderá a la recepción en los dispositivos de comunicaciones electrónicas del investigado de cualquier dato de verificación necesarios para el acceso a los equipos o dispositivos investigados.

5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en responsabilidad penal.

Esta disposición no será aplicable al investigado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que no pueden declarar en virtud del secreto profesional.

Artículo 36. Incautación de equipos y dispositivos

Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

Sección Segunda
Registro remoto de equipos informáticos y telemáticos

Artículo 37. Presupuestos

La autoridad podrá autorizar por el plazo de un mes, prorrogable por iguales períodos hasta un máximo de tres, la utilización de datos de identificación y códigos, así como la instalación de cualquier programa o aplicación que permita, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos de organización criminal o cometidos en el seno de organizaciones criminales.

b) Delitos cometidos contra menores o personas con capacidad modificada.

c) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

d) Delitos castigados con pena privativa de libertad de al menos dos años de prisión.

Artículo 38. Resolución

1. La resolución que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

d) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

2. En los supuestos en los que, durante la ejecución de la medida, surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema informático, se podrá extender o ampliar el registro al otro sistema. La ampliación del registro deberá ser autorizada, salvo que estuviera prevista en la orden original.

Artículo 39. Control de la medida

1. La autoridad encargada de su ejecución informará a quien autorizó la medida de los resultados obtenidos cada quince días.

2. La herramienta informática empleada para la ejecución de la medida será certificada por el organismo estatal encargado de la ciberseguridad de modo que garantice el alcance de las utilidades implementadas y su coherencia con la resolución autorizante.

Únicamente será posible someter a dictamen pericial el correcto funcionamiento de la herramienta empleada.

Artículo 40. Duración de la medida

La medida a que se refiere esta Sección tendrá una duración de un mes, con posibilidad de prórrogas por iguales períodos hasta un máximo de tres meses.

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

EL PAcCTO es un programa de cooperación internacional financiado por la Unión Europea que persigue promover la seguridad ciudadana y el Estado de derecho en América Latina a través de una lucha más efectiva contra el crimen transnacional organizado y de una cooperación fortalecida en la materia. Cubre los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela. Es la primera vez que un programa regional europeo trabaja en toda la cadena penal para fortalecer la cooperación a través de tres componentes (cooperación policial, cooperación entre sistemas de justicia y sistemas penitenciarios) con cinco ejes transversales (cibercrimen, corrupción, derechos humanos, género y lavado de activos).

Programa liderado por

FIIAPP COOPERACIÓN ESPAÑOLA

EXPERTISE FRANCE

Socios coordinadores

iila

CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL

PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA