LEY 9/2014, DE 9 DE MAYO, GENERAL DE TELECOMUNICACIONES

DISPOSICIONES GENERALES (Tít. 1)

Objeto y ámbito de aplicación de la Ley (Art. 1)

El objeto de esta ley es la **regulación** de las **telecomunicaciones**, que comprende la [1]**instalación** y **explotación** de las **redes** de **comunicaciones electrónicas**, la [2]**prestación** de los **servicios** de **comunicaciones electrónicas**, sus **recursos** y **servicios asociados**, los **equipos radioeléctricos** y los **equipos terminales** de **telecomunicación**, de conformidad con el art. 149.1.21ª de la Constitución.

En particular, esta ley es de **aplicación** al **dominio público radioeléctrico** **utilizado** por parte de **todas** las **redes de comunicaciones electrónicas**, ya sean **públicas** o **no**, y con independencia del servicio que haga uso del mismo.

Quedan **excluidos** del ámbito de esta ley los [1]**servicios** de **comunicación audiovisual**, los [2]**servicios** de **intercambio de vídeos** a través de **plataforma**, los [3]**contenidos audiovisuales** transmitidos a través de las **redes**, así como el [4]**régimen básico** de los **medios de comunicación social** de **naturaleza audiovisual** a que se refiere el artículo 149.1.27.ª de la Constitución.

Asimismo, se **excluyen** del ámbito de esta ley los [5]**servicios** que **suministren contenidos** transmitidos mediante **redes** y **servicios** de **comunicaciones electrónicas**, las [6]**actividades** que consistan en el ejercicio del **control editorial** sobre dichos **contenidos** y los [7]**servicios** de la **Sociedad de la Información**, regulados en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en tanto en cuanto **no** sean asimismo **servicios** de **comunicaciones electrónicas**.

Las telecomunicaciones como servicios de interés general (Art. 2)

Las **telecomunicaciones** son **servicios** de **interés general** que se prestan en **régimen** de **libre competencia**.

Sólo tienen la consideración de servicio público o están sometidos a obligaciones de servicio público los servicios regulados en el artículo 4 y en el título III, respectivamente.

Objetivos y principios de la ley (Art. 3)

Los **objetivos** y **principios** de esta ley son los siguientes:

- **Fomentar** la **competencia** **efectiva** y **sostenible** en los mercados de **telecomunicaciones** para **potenciar** al máximo los **intereses** y **beneficios** para las **empresas** y los **consumidores**, principalmente en términos de [1]**bajada** de los **precios**, [2]**calidad** de los **servicios**, [3]**variedad** de **elección** e **innovación**, teniendo debidamente **en cuenta** la variedad de **condiciones** en cuanto a la **competencia** y los **consumidores** que existen en las distintas **áreas geográficas**, y velando por que **no** exista **falseamiento** ni **restricción** de la competencia en la **explotación de redes** o en la prestación de **servicios de comunicaciones electrónicas**, incluida la transmisión de contenidos:

- **Desarrollar** la **economía** y el **empleo digital**, **promover** el **desarrollo** del sector de las **telecomunicaciones** y de todos los **nuevos servicios digitales** que las nuevas **redes** de alta y muy alta capacidad **permiten**, **impulsando** la **cohesión social** y **territorial**, mediante la **mejora** y **extensión** de las **redes**, especialmente las de **muy alta capacidad**, así como la **prestación** de los **servicios de comunicaciones electrónicas** y el **suministro** de los **recursos asociados** a ellas;

- **Promover**, en aras a la consecución del fin de interés general que supone, el **despliegue de redes** y la **prestación** de **servicios de comunicaciones electrónicas**, **fomentando** la [1]**conectividad**, el [2]**acceso** a las **redes** de **muy alta capacidad**, incluidas las **redes fijas**, **móviles** e **inalámbricas** y la [3]**interoperabilidad** de **extremo a extremo**, en condiciones de **igualdad** y **no discriminación**;

- **Impulsar** la **innovación** en el **despliegue de redes** y la **prestación** de **servicios de comunicaciones**, en aras a garantizar el **servicio universal** y la **reducción de la desigualdad** en el **acceso** a **internet** y las **Tecnologías de la Información y la Comunicación** (TIC), con especial consideración al **despliegue de redes** y **servicios a la ciudadanía** vinculados a la **mejora** del [1]**acceso funcional a internet**, del [2]**teletrabajo**, del [3]**medioambiente**, de la [4]**salud** y la **seguridad públicas** y de la [5]**protección civil**; así como cuando **faciliten** la **vertebración** y **cohesión social** y **territorial** o contribuyan a la **sostenibilidad** de la **logística urbana**.

- Promover el **desarrollo** de la **ingeniería**, así como de la **industria de productos** y **equipos de telecomunicaciones**;

- Contribuir al **desarrollo** del **mercado interior** de **servicios de comunicaciones electrónicas** en la **Unión Europea**, **facilitando** la convergencia de las condiciones que permitan la **inversión** en **redes de comunicaciones electrónicas** y en su **suministro**, en **servicios de comunicaciones electrónicas**, en **recursos asociados** y **servicios asociados** en toda la **Unión**;

- **Promover** la **inversión eficiente** en materia de **infraestructuras**, especialmente en las **redes** de **muy alta capacidad**, **incluyendo**, cuando proceda y con carácter prioritario, la **competencia** basada en **infraestructuras**, **reduciendo** progresivamente la **intervención ex ante** en los **mercados**, **posibilitando** la **coinversión** y el **uso compartido** y **fomentando** la **innovación**, teniendo debidamente en cuenta los riesgos en que incurren las empresas inversoras;

- Hacer posible el **uso eficaz** y **eficiente** de los **recursos limitados** de **telecomunicaciones**, como la **numeración** y el **espectro radioeléctrico**, la adecuada **protección** de este último, y el **acceso** a los **derechos de ocupación** de la **propiedad pública** y **privada**;

- **Fomentar** la **neutralidad tecnológica** en la regulación;

- **Garantizar** el **cumplimiento** de las obligaciones de **servicio público** en la **explotación de redes** y la **prestación** de **servicios** de **comunicaciones electrónicas** a las que se refiere el título III, en especial las de **servicio universal**;

- **Defender** los **intereses** de los **usuarios**, asegurando su **derecho** al **acceso** a los **servicios** de **comunicaciones electrónicas** en **condiciones** adecuadas de **elección**, **precio** y **buena calidad**, promoviendo la **capacidad** de los **usuarios finales** para **acceder** y **distribuir** la **información** o utilizar las aplicaciones y los servicios de su elección, en particular a través de un **acceso abierto** a **internet**. En la prestación de estos servicios deben **salvaguardarse** los imperativos constitucionales de [1]**no discriminación**, de [2]**respeto** a los [3]**derechos** al **honor** y a la **intimidad**,

la [4]**protección** a la **juventud** y a la **infancia**, la [5]**protección** a las **personas con discapacidad**, la [6]**protección** de los **datos personales** y el [7]**secreto** en las **comunicaciones**;

- **Salvaguardar** y **proteger** en los **mercados** de telecomunicaciones la **satisfacción** de las **necesidades** de **grupos sociales específicos**, las **personas con discapacidad**, las **personas mayores**, las personas **en situación de dependencia** y usuarios **con necesidades sociales especiales**, atendiendo a los **principios** de **igualdad de oportunidades** y **no discriminación**. En lo relativo al acceso a los servicios de comunicaciones electrónicas de las personas con discapacidad y personas en situación de dependencia, se fomentará el cumplimiento de las normas o las especificaciones pertinentes relativas a normalización técnica publicadas de acuerdo con la normativa comunitaria y se facilitará el acceso de los usuarios con discapacidad a los servicios de comunicaciones electrónicas y al uso de equipos terminales;

- **Impulsar** la **universalización** del **acceso** a las **redes** y **servicios** de **comunicaciones electrónicas** de **banda ancha** y contribuir a alcanzar la **mayor vertebración territorial** y **social** posible mediante el **despliegue de redes** y la **prestación** de **servicios de comunicaciones electrónicas** en las distintas zonas del **territorio español**, especialmente en aquellas que necesitan de la instalación de redes de comunicaciones electrónicas y la mejora de las existentes para permitir impulsar distintas actividades económicas y sociales.

Servicios de telecomunicaciones para la seguridad nacional, la defensa nacional, la seguridad pública, la seguridad vial y la protección civil (Art. 4)

Sólo tienen la **consideración** de **servicio público** los **servicios** regulados en **este artículo**.

Las **redes**, **servicios**, **instalaciones** y **equipos de telecomunicaciones** que desarrollen **actividades esenciales** para la **seguridad** y **defensa nacionales** integran los medios destinados a éstas, se **reservan** al **Estado** y se **rigen** por su **normativa específica**.

El **Ministerio de Asuntos Económicos y Transformación Digital** es el **órgano** de la **Administración General del Estado** con competencia, de conformidad con la legislación específica sobre la materia y lo establecido en esta ley, para **ejecutar**, en la medida en que le afecte, la **política de defensa nacional** en el sector de las **telecomunicaciones**, con la debida **coordinación** con el **Ministerio de Defensa** y siguiendo los **criterios** fijados por éste.

En el marco de las **funciones** relacionadas con la **defensa civil**, **corresponde** al **Ministerio de Asuntos Económicos y Transformación Digital** **estudiar**, **planear**, **programar**, **proponer** y **ejecutar** cuantas **medidas** se relacionen con su aportación a la **defensa nacional** en el ámbito de las **telecomunicaciones**.

A tales efectos, los **Ministerios** de **Defensa** y de **Asuntos Económicos y Transformación Digital** **coordinarán** la **planificación** del **sistema de telecomunicaciones** de las **Fuerzas Armadas**, a fin de **asegurar**, en la medida de lo posible, su **compatibilidad** con los **servicios civiles**. Asimismo, **elaborarán** los **programas de coordinación tecnológica** precisos que faciliten la **armonización**, **homologación** y **utilización**, conjunta o indistinta, de los **medios**, **sistemas** y **redes civiles** y **militares** en el ámbito de las telecomunicaciones. Para el estudio e informe de estas materias, se constituirán los órganos interministeriales que se consideren adecuados, con la composición y competencia que se determinen mediante real decreto.

En los ámbitos del **orden público**, la **seguridad pública**, **seguridad vial** y de la **protección civil**, en su específica relación con el uso de las telecomunicaciones, el **Ministerio de Asuntos Económicos y Transformación Digital** **cooperará con** el **Ministerio del Interior** y con los **órganos responsables** de las **Comunidades Autónomas** con **competencias** sobre las citadas materias.

Los **bienes** **muebles** o **inmuebles** **vinculados** a los **centros**, **establecimientos** y **dependencias** afectos a la **instalación** y **explotación** de las **redes** y a la **prestación** de los **servicios de comunicaciones electrónicas** dispondrán de las **medidas** y **sistemas** de **seguridad**, **vigilancia**, **difusión de información**, **prevención de riesgos** y **protección** que se **determinen** por el **Gobierno**, a **propuesta** de los **Ministerios** de **Defensa**, del **Interior** o de **Asuntos Económicos y Transformación Digital**, dentro del ámbito de sus respectivas competencias. Estas medidas y sistemas deberán estar disponibles en las situaciones de normalidad o en las de crisis, así como en los supuestos contemplados en la Ley Orgánica 4/1981, de 1 de junio, reguladora de los Estados de Alarma, Excepción y Sitio, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil y el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

El **Gobierno**, con **carácter** **excepcional** y **transitorio**, podrá acordar la **asunción** por la **Administración General del Estado** de la **gestión directa** de determinados **servicios de comunicaciones electrónicas disponibles al público**, distintos de los servicios de comunicaciones interpersonales, independientes de la numeración o de la explotación de ciertas redes públicas de comunicaciones electrónicas, para **garantizar** la **seguridad pública** y la **seguridad nacional**, en los términos en que dichas redes y servicios están definidos en el anexo II, **excluyéndose** en consecuencia las **redes** y **servicios** que se **exploten** o **presten** íntegramente en **autoprestación**. Esta facultad excepcional y transitoria de gestión directa podrá **afectar** a **cualquier infraestructura**, **recurso asociado** o **elemento** o **nivel** de la **red** o del **servicio** que resulte necesario para **preservar** o **restablecer** la **seguridad pública** y la **seguridad nacional**.

En ningún caso esta **intervención** podrá suponer una **vulneración** de los **derechos fundamentales** y **libertades públicas** reconocidas en el **ordenamiento jurídico**.

Asimismo, en el caso de **incumplimiento** de las **obligaciones** de **servicio público** a las que se refiere el título III, el **Gobierno**, previo **informe preceptivo** de la **Comisión Nacional de los Mercados** y la **Competencia**, e igualmente con **carácter excepcional** y **transitorio**, podrá acordar la **asunción** por la **Administración General del Estado** de la **gestión directa** de los correspondientes **servicios** o de la **explotación** de las correspondientes **redes**. En este último caso, podrá, con las **mismas condiciones**, intervenir la prestación de los servicios de **comunicaciones electrónicas**.

Los **acuerdos** de [1]**asunción** de la **gestión directa** del **servicio** y de [2]**intervención** de este o los de [3]**intervenir** o **explotar** las **redes** a los que se refieren los párrafos anteriores **se adoptarán por** el **Gobierno** por **propia iniciativa** o a **instancia** de una **Administración Pública competente**. En este último caso, será preciso que la **Administración Pública** tenga **competencias** en materia de **seguridad** o para la **prestación** de los **servicios públicos afectados** por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el **procedimiento** se inicie **a instancia** de una **Administración distinta** de la del **Estado**, aquella tendrá la **consideración** de **interesada** y podrá **evacuar informe** con carácter **previo** a la **resolución final**.

Los **acuerdos** de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refiere este apartado deberán ser **comunicados** por el **Gobierno** en el plazo de **24 horas** al **órgano jurisdiccional** competente para que, en un plazo de **48 horas**, establezca si los mismos resultan **acordes** con los **derechos fundamentales** y **libertades públicas** reconocidas en el ordenamiento jurídico, procediendo a su **anulación** en **caso negativo**.

La **regulación** contenida en esta **ley** se entiende **sin perjuicio** de lo previsto en la **normativa específica** sobre las **telecomunicaciones** relacionadas con el **orden público**, la **seguridad pública**, la **defensa nacional** y la **seguridad nacional**.

CAPÍTULO 3

Salvaguardia de derechos fundamentales, secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas

Salvaguardia de derechos fundamentales (Art. 56)

Las **medidas** que se adopten en relación al **acceso** o al **uso** por parte de los **usuarios finales** de los **servicios** y las **aplicaciones** a través de redes de comunicaciones electrónicas **respetarán** los **derechos** y **libertades fundamentales**, como queda **garantizado** en el [1]**Convenio Europeo** para la **Protección de los Derechos Humanos** y de las **Libertades Fundamentales**, en la [2]**Carta de Derechos Fundamentales** de la Unión Europea, en los [3]**principios generales** del **Derecho comunitario** y en la **Constitución Española**.

Cualquiera de esas **medidas** relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea **susceptible** de **restringir** esos **derechos** y **libertades fundamentales** solo podrá **imponerse** si es **adecuada**, **necesaria** y **proporcionada** en una **sociedad democrática**, y su **aplicación** está **sujeta** a las **salvaguardias de procedimiento** apropiadas de conformidad con las normas mencionadas en el apartado anterior. Por tanto, dichas medidas **solo** podrán ser **adoptadas respetando** debidamente el [1]**principio** de **presunción de inocencia**, el [2]**derecho** a la **vida privada** e **intimidad**, el [3]**derecho** a la **libertad de expresión** e **información** y el [4]**derecho** a la **tutela judicial efectiva**, a través de un procedimiento previo, justo e imparcial, que **incluirá** el **derecho** de los interesados **a ser oídos**, **sin perjuicio** de que concurran las **condiciones** y los **requisitos** procedimentales adecuados en los **casos de urgencia** debidamente justificados, de conformidad con el **Convenio Europeo** para la Protección de los Derechos Humanos y Libertades Fundamentales y la **Carta de los Derechos Fundamentales** de la Unión Europea.

Principio de no discriminación (Art. 57)

Los **operadores** que **instalen** o **exploten redes públicas** de comunicaciones electrónicas o que **presten servicios** de comunicaciones electrónicas disponibles al público **no aplicarán** a los **usuarios finales** ningún **requisito diferente** ni **condiciones generales** de **acceso** o **uso** de redes o servicios ni de **utilización** de los mismos por **motivos** relacionados con la [1]**nacionalidad**, el [2]**lugar de residencia** o el [3]**lugar** de **establecimiento del usuario final**, a menos que dicho trato diferente se justifique de forma objetiva.

Secreto de las comunicaciones (Art. 58)

Los **operadores** que **suministren redes públicas** de **comunicaciones electrónicas** o que **presten servicios** de comunicaciones electrónicas disponibles al público deberán **garantizar** el **secreto de las comunicaciones** de conformidad con los art. 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

Los **operadores** que **suministren redes públicas** de comunicaciones electrónicas o que **presten servicios** de **comunicaciones interpersonales** basados en **numeración disponibles al público** o **servicios** de **acceso a internet** están **obligados** a realizar las **interceptaciones** que se autoricen judicialmente de acuerdo con lo establecido en el cap. 5 del título 8 del libro 2 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán **adoptar a su costa** las **medidas** que se establecen en este artículo y en los **reglamentos** correspondientes.

La **interceptación** a que se refiere el apartado anterior deberá **facilitarse** para cualquier **comunicación** que tenga como origen o destino el **punto de terminación** de **red** o el **terminal específico** que se determine **a partir de** la **orden de interceptación legal**, **incluso** aunque esté **destinada** a **dispositivo de almacenamiento** o **procesamiento de la información**; asimismo, la **interceptación** podrá realizarse sobre un **terminal conocido** y con unos **datos de ubicación temporal** para comunicaciones desde locales públicos. Cuando **no** exista una **vinculación fija** entre el **sujeto** de la interceptación y el **terminal** utilizado, éste podrá ser **determinado** dinámicamente cuando el **sujeto** de la interceptación **lo active** para la comunicación mediante un **código de identificación personal**.

El **acceso** se facilitará para **todo tipo** de **comunicaciones electrónicas** disponibles al público **distintas** de las **comunicaciones interpersonales independientes** de la **numeración**, en particular, por su **penetración** y **cobertura**, para las que se realicen mediante **cualquier modalidad** de los servicios de **telefonía** y de **transmisión de datos**, se trate de comunicaciones de **vídeo**, **audio**, **intercambio** de **mensajes**, **ficheros** o de la **transmisión de facsímiles**.

El **acceso facilitado** servirá tanto para la **supervisión** como para la **transmisión** a los **centros de recepción** de las interceptaciones de la comunicación electrónica interceptada y la **información relativa** a la interceptación, y **permitirá obtener** la **señal** con la que se realiza la comunicación.

Los **sujetos obligados** deberán **facilitar** al **agente facultado**, salvo que por las características del servicio no estén a su disposición, los **datos** indicados en la **orden de interceptación legal**, de entre los que se relacionan a continuación:

- **Identidad** o identidades del **sujeto** objeto de la medida de la interceptación. Se entiende por **identidad**: **etiqueta técnica** que puede representar el **origen** o el **destino** de cualquier **tráfico** de comunicaciones electrónicas, en general **identificada** mediante un **número de identidad** de **comunicaciones electrónicas** **físico** (tal como un número de teléfono) o un **código de identidad** de **comunicaciones electrónicas** **lógico** o **virtual** (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

  Los **sujetos obligados proporcionarán**, cuando técnicamente sea posible, los **identificadores permanentes** que sean necesarios para la **atribución** de un **servicio** a un **usuario** determinado de forma inequívoca, así como los **identificadores** del **dispositivo empleado** para la

comunicación. Si en una comunicación electrónica se asignaran identidades de carácter temporal al usuario, el sujeto obligado implementará, cuando técnicamente sea posible, las medidas de correlación necesarias para que en la información de la interceptación se faciliten las identidades permanentes que permitan la identificación inequívoca del usuario asignado, así como del dispositivo empleado en la comunicación.

- **Identidad** o identidades de las **otras partes involucradas** en la comunicación electrónica;
- **Servicios básicos** utilizados;
- **Servicios suplementarios** utilizados;
- **Dirección** de la **comunicación**;
- **Indicación** de **respuesta**;
- **Causa** de **finalización**;
- **Marcas temporales**;
- **Información** de **localización**;
- **Información intercambiada** a través del **canal de control** o **señalización**.

Además de la información relativa a la interceptación prevista en el apartado anterior, los **sujetos obligados** deberán **facilitar** al **agente facultado**, salvo que por las características del servicio no estén a su disposición, de **cualquiera** de las **partes** que **intervengan** en la comunicación que sean **clientes** del **sujeto obligado**, los siguientes **datos**:

- **Identificación** de la **persona física** o **jurídica**;
- **Domicilio** en el que el operador realiza las **notificaciones**; y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:
- **Número** de **titular** de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado);
- **Número** de identificación del **terminal**;
- **Número** de **cuenta** asignada por el proveedor de servicios internet;
- **Dirección** de **correo electrónico**.

Junto con los datos previstos en los apartados anteriores, los **sujetos obligados** deberán **facilitar**, salvo que por las características del servicio no esté a su disposición, **información** de la **situación geográfica** del **terminal** o **punto de terminación** de red **origen** de la llamada, y de la del **destino de la llamada**. En caso de **servicios móviles**, se proporcionará una **posición** lo **más exacta posible** del **punto de comunicación** y, en todo caso, la **identificación**, **localización** y **tipo** de la **estación base** afectada.

Los **sujetos obligados** deberán **facilitar** al agente facultado, de entre los datos previstos en los apdos. 5, 6 y 7 de este artículo, **sólo** aquéllos que estén **incluidos** en la **orden de interceptación legal**.

Con carácter **previo** a la **ejecución** de la **orden de interceptación legal**, los **sujetos** obligados deberán **facilitar** al **agente** facultado **información** sobre los **servicios** y **características** del **sistema**

de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes **nombres** de los **abonados** con sus **números** de **documento nacional de identidad**, **tarjeta de identidad de extranjero** o **pasaporte**, en el caso de personas físicas, o denominación y **número** de **identificación fiscal** en el caso de **personas jurídicas**.

Los **sujetos obligados** deberán tener en todo momento **preparadas una** o **más interfaces** a través de las cuales las **comunicaciones electrónicas interceptadas** y la **información** relativa a la interceptación se **transmitirán** a los **centros de recepción** de las **interceptaciones**. Las **características** de estas **interfaces** y el **formato** para la **transmisión** de las comunicaciones interceptadas a estos centros estarán **sujetas** a las **especificaciones técnicas** que se establezcan por el **Ministerio de Asuntos Económicos y Transformación** Digital.

En el caso de que los **sujetos obligados apliquen** a las comunicaciones objeto de interceptación legal algún **procedimiento** de **compresión**, **cifrado**, **digitalización** o cualquier **otro tipo** de codificación, deberán **entregar** aquellas **desprovistas** de los efectos de tales **procedimientos**, siempre que sean **reversibles**.

Las **comunicaciones interceptadas** deben proveerse al centro de recepción de las interceptaciones con una **calidad no inferior** a la que **obtiene** el **destinatario** de la **comunicación**.

Interceptación de las comunicaciones electrónicas por los servicios técnicos. (Art. 59)

Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la **realización** de las tareas de **control** para la eficaz utilización del **dominio público radioeléctrico** o para la **localización** de **interferencias perjudiciales** sea necesaria la utilización de **equipos**, **infraestructuras** e **instalaciones técnicas** de **interceptación de señales** no dirigidas al público en general, será de **aplicación** lo siguiente:

- La **administración** de las telecomunicaciones deberá diseñar y establecer sus **sistemas técnicos** de **interceptación de señales** en forma tal que se **reduzca** al mínimo el **riesgo** de **afectar** a los **contenidos** de las comunicaciones;
- Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los **soportes** en los que éstos aparezcan deberán ser **custodiados hasta** la **finalización**, en su caso, del **expediente sancionador** que hubiera lugar o, en otro caso, **destruidos** inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

Las **mismas reglas** se aplicarán para la **vigilancia** del adecuado **empleo** de las **redes** y la correcta **prestación** de los **servicios** de comunicaciones electrónicas.

Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el art. 85.

Protección de los datos de carácter personal (Art. 60)

Los **operadores** que **suministren redes públicas** de comunicaciones electrónicas o que **presten servicios** de comunicaciones electrónicas disponibles **al público**, **incluidas** las **redes públicas** de comunicaciones que **den soporte** a **dispositivos** de **identificación** y **recopilación de datos**, deberán

adoptar las **medidas técnicas** y **de gestión** adecuadas para **preservar** la **seguridad** en el **suministro** de su **red** o en la **prestación** de sus **servicios**, con el fin de garantizar la protección de los datos de carácter personal. Dichas **medidas** incluirán, como mínimo:

- La **garantía** de que **sólo** el **personal autorizado** tenga **acceso** a los **datos personales** para fines autorizados por la ley;
- La **protección** de los **datos personales almacenados** o **transmitidos** de la **destrucción accidental** o **ilícita**, la **pérdida** o **alteración accidentales** o el **almacenamiento**, **tratamiento**, **acceso** o **revelación no autorizados** o **ilícitos**;
- La **garantía** de la aplicación efectiva de una **política de seguridad** con respecto al **tratamiento** de **datos personales**.

La **Agencia Española de Protección de Datos**, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá **examinar** las **medidas adoptadas** por los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá **formular recomendaciones** sobre las **mejores prácticas** con respecto al **nivel de seguridad** que debería **conseguirse** con estas medidas.

En caso de que exista un **riesgo particular** de **violación de la seguridad** de la **red pública** o del **servicio de comunicaciones electrónicas**, el **operador** que suministre dicha red o preste el servicio de comunicaciones electrónicas **informará** a los **abonados** sobre dicho **riesgo** y sobre las **medidas** a adoptar.

En caso de **violación** de los **datos personales**, el **operador** de servicios de comunicaciones electrónicas disponibles al público **notificará sin dilaciones** indebidas dicha violación a la **Agencia Española de Protección de Datos**. Si la **violación** de los datos pudiera **afectar negativamente** a la **intimidad** o a los **datos personales** de un abonado o particular, el operador notificará **también** la violación al **abonado** o **particular sin dilaciones** indebidas.

La **notificación** de una **violación** de los datos personales a un **abonado** o **particular** afectado **no** será **necesaria** si el **operador ha probado a satisfacción** de la **Agencia Española de Protección de Datos** que ha aplicado las **medidas de protección tecnológica** convenientes y que estas medidas **se han aplicado** a los **datos afectados** por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Sin perjuicio de la obligación del operador de informar a los abonados o particulares afectados, si el **operador no** ha **notificado ya** al **abonado** o al **particular** la violación de los datos personales, la **Agencia Española de Protección de Datos** podrá **exigirle** que lo haga, una vez **evaluados** los posibles **efectos adversos** de la violación.

En la **notificación** al **abonado** o al **particular** se **describirá** al menos la **naturaleza** de la **violación** de los **datos personales** y los **puntos de contacto** donde puede **obtenerse más información** y se recomendarán **medidas** para **atenuar** los posibles **efectos** adversos de dicha violación. En la notificación a la **Agencia Española de Protección de Datos** se **describirán** además las **consecuencias** de la **violación** y las **medidas propuestas** o **adoptadas** por el **operador** respecto a la violación de los datos personales.

Los **operadores** deberán llevar un **inventario** de las **violaciones** de los datos personales, **incluidos** los **hechos relacionados** con tales infracciones, sus **efectos** y las **medidas adoptadas** al respecto, que resulte suficiente para **permitir** a la **Agencia Española de Protección de Datos verificar** el cumplimiento de las **obligaciones de notificación** reguladas en este apartado. Mediante **real decreto** podrá establecerse el **formato** y **contenido** del inventario.

A los efectos establecidos en este artículo, **se entenderá** como **violación** de los **datos personales** la **violación** de la **seguridad** que **provoque** la [1]**destrucción**, accidental o ilícita, la [2]**pérdida**, la [3]**alteración**, la [4]**revelación** o el [5]**acceso no autorizados**, de **datos personales transmitidos**, **almacenados** o **tratados de otro modo** en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La **Agencia Española de Protección de Datos** podrá **adoptar directrices** y, en caso necesario, **dictar instrucciones** sobre las [1]**circunstancias** en que se requiere que el **operador notifique** la **violación** de los **datos** personales, sobre el [2]**formato** que debe adoptar dicha **notificación** y sobre la [3]**manera** de **llevarla a cabo**, con pleno **respeto** a las **disposiciones** que en su caso sean adoptadas en esta materia por la **Comisión Europea**.

Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Art. 61)

La **conservación** y **cesión** de los **datos** generados o tratados en el marco de la prestación de **servicios de comunicaciones electrónicas** o de **redes públicas** de comunicación a los **agentes facultados** a través de la correspondiente **autorización judicial** con fines de **detección**, **investigación** y **enjuiciamiento** de **delitos graves** contemplados en el Código Penal o en las leyes penales especiales **se rige por** lo establecido en la **Ley 25/2007**, de 18 de octubre, de **conservación** de **datos** relativos a las **comunicaciones electrónicas** y a las **redes públicas** de comunicaciones.

Cifrado en las redes y servicios de comunicaciones electrónicas (Art. 62)

Cualquier tipo de **información** que se **transmita** por **redes** de **comunicaciones electrónicas** podrá ser **protegida** mediante **procedimientos** de **cifrado**.

El **cifrado** es un **instrumento de seguridad** de la **información**. Entre sus condiciones de uso, cuando se utilice para **proteger** la **confidencialidad** de la información, se podrá imponer la [1]**obligación** de **facilitar** a un **órgano** de la **Administración General del Estado** o a un **organismo público**, los **algoritmos** o cualquier **procedimiento de cifrado** utilizado, en casos justificados de **protección** de los **intereses** esenciales de **seguridad** del **Estado** y la **seguridad pública**, y para **permitir** la **investigación**, la **detección** y el **enjuiciamiento** de **delitos**, así como la [2]obligación de **facilitar** sin coste alguno los **aparatos de cifra** a efectos de su **control** de acuerdo con la normativa vigente.

Toda **información obtenida** por parte de la Administración General del Estado o cualquier organismo público **a través** de los **preceptos** incluidos en el apartado 2 de este artículo deberá ser **tratada** con la **máxima confidencialidad** y **destruida** una vez que se **resuelva** la **amenaza** para la **seguridad del Estado** y la **seguridad pública** o se haya dictado **sentencia firme** sobre el **delito** en cuestión.

Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas (Art. 63)

Los **operadores** de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público, **gestionarán** adecuadamente los **riesgos de seguridad** que puedan afectar a sus redes y servicios a fin de **garantizar** un adecuado nivel de **seguridad** y **evitar** o **reducir** al mínimo el **impacto** de los **incidentes de seguridad** en los **usuarios** y en **otras redes** y **servicios**, para lo cual deberán **adoptar** las **medidas técnicas** y **organizativas** adecuadas, que deberán ser **proporcionadas** y **en línea** con el **estado de la técnica**, pudiendo incluir el **cifrado**.

Asimismo, los **operadores** de redes públicas de comunicaciones electrónicas **garantizarán** la **integridad** de las mismas a fin de **asegurar** la **continuidad** en la prestación de los **servicios** que utilizan dichas redes.

Los **operadores** que suministren redes públicas o presten servicios de comunicaciones electrónicas disponibles al público **notificarán** al **Ministerio de Asuntos Económicos y Transformación Digital** los **incidentes de seguridad** que hayan tenido un **impacto significativo** en el **suministro** de las **redes** o los **servicios**.

Con el fin de **determinar** la **importancia** del impacto de un **incidente de seguridad** se tendrán en cuenta, en particular, los **parámetros** siguientes, cuando se disponga de ellos:

- El **número** de **usuarios afectados** por el incidente de seguridad;
- La **duración** del **incidente** de seguridad;
- El **área geográfica** **afectada** por el incidente de seguridad;
- La **medida** en que se ha visto **afectado** el **funcionamiento** de la red o del servicio;
- El **alcance del impacto** sobre las **actividades económicas** y **sociales**.

Cuando proceda, el **Ministerio informará** a las **autoridades nacionales** competentes **de otros Estados miembros** y a la **Agencia Europea de Seguridad en las Redes y la Información** (ENISA). Asimismo, podrá **informar** al **público** o **exigir** a los **operadores que lo hagan**, en caso de estimar que la divulgación del **incidente** de seguridad reviste **interés público**. **Una vez al año**, el **Ministerio presentará** a la **Comisión** y a la **ENISA** un **informe resumido** sobre las **notificaciones** recibidas y las **medidas** adoptadas de conformidad con este apartado.

Del mismo modo, el **Ministerio comunicará** a la **Secretaría de Estado de Seguridad** del **Ministerio del Interior** aquellos **incidentes** que afectando a los **operadores estratégicos nacionales** sean de **interés** para la **mejora** de la **protección de infraestructuras críticas**, en el marco de la Ley 8/2011, de 28 de abril, reguladora de las mismas. También el **Ministerio comunicará** a la **Comisión Nacional de los Mercados y la Competencia** los **incidentes de seguridad** a que se refiere este apartado que

afecten o **puedan afectar** a las **obligaciones** específicas **impuestas** por dicha Comisión en los **mercados de referencia**.

En caso de que exista una **amenaza particular** y **significativa** de **incidente de seguridad** en las redes públicas de comunicaciones electrónicas o en los servicios de comunicaciones electrónicas disponibles para el público, los **operadores** deberán **informar** a sus **usuarios** que pudieran **verse afectados** por dicha amenaza sobre las posibles **medidas de protección** o **soluciones** que pueden adoptar los usuarios. Cuando proceda, los operadores también **informarán** a sus **usuarios** sobre la **propia amenaza**.

El **Ministerio de Asuntos Económicos y Transformación Digital** establecerá los mecanismos para **supervisar** el cumplimiento de las **obligaciones** anteriores y, en su caso, **dictará** las **instrucciones** correspondientes, que serán **vinculantes** para los **operadores**, incluidas las relativas a las medidas necesarias adicionales a las identificadas por los operadores para solventar incidentes de seguridad, o impedir que ocurran cuando se haya observado una amenaza significativa, e incumplimientos de las fechas límite de aplicación. Entre las **medidas relativas** a la **integridad** y **seguridad** de redes y servicios de comunicaciones electrónicas que se puedan **exigir a** los **operadores**, podrá **imponer**:

- La obligación de **facilitar** la **información necesaria** para **evaluar** la **seguridad** y la **integridad** de sus servicios y redes, **incluidos** los **documentos** sobre las **políticas de seguridad**;
- La obligación de **someterse** a una **auditoría de seguridad** realizada por un **organismo independiente** o por una **autoridad** competente, y de poner el **resultado** a disposición del **Ministerio de Asuntos Económicos y Transformación Digital**. El **coste** de la auditoría será sufragado por el **operador**.

En particular, los **operadores** garantizarán la **mayor disponibilidad posible** de los **servicios** de comunicaciones vocales y de acceso a internet **a través de** las **redes públicas de comunicaciones electrónicas** en caso de [1]**fallo catastrófico** de la red o en casos de [2]**fuerza mayor**, y adoptarán todas las **medidas** necesarias para garantizar el **acceso sin interrupciones** a los **servicios** de **emergencia** y la **transmisión ininterrumpida** de las **alertas públicas**.

El presente artículo se entiende sin perjuicio de lo establecido en el artículo 4.6.

Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo.