

Lección 16: Los Actos de Investigación Restrictivos de Derechos Fundamentales en el Ámbito Electrónico

Derecho Procesal Penal — Medidas de Investigación Tecnológica. Estudio de las medidas de investigación tecnológica reguladas en la [LO 13/2015, de 5 de octubre](#), de modificación de la Ley de Enjuiciamiento Criminal, con especial atención a la protección de los derechos fundamentales del investigado en el entorno digital.

LECCIÓN 16

LECRIM — TÍTULO VIII, LIBRO II



Índice de Contenidos

01

I. Intimidad en el Entorno Virtual

El derecho al entorno digital y la autodeterminación informativa como derechos de nueva generación.

02

II. Disposiciones Generales

Principios rectores de las medidas de investigación tecnológica: legalidad, especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

03

III–VII. Las Medidas en Particular

Interceptación de comunicaciones, captación oral, captación de imagen, seguimiento y localización, registro de dispositivos y registro remoto.

04

VIII. Conservación de Datos

Orden de conservación de datos archivados y su régimen jurídico.

05

Casos Prácticos I–VI

Corrección razonada de los seis casos prácticos conforme a los apuntes y a la LECrim.

I. Actos de Investigación Electrónicos: La Intimidad en su Doble Proyección

La proliferación de dispositivos electrónicos capaces de acumular ingentes cantidades de datos personales ha obligado al Tribunal Supremo a proclamar la existencia de un nuevo derecho fundamental: el **derecho al entorno digital**. Este derecho de última generación actúa como paraguas protector de la intimidad digital individual frente a las injerencias de terceros y de los propios poderes públicos.

Derecho al Entorno Digital

Se integra toda la información generada por el usuario de la red, consciente o inconscientemente, a través del uso de las nuevas tecnologías. Navegar por Internet, participar en redes sociales, descargar archivos o realizar operaciones de comercio electrónico genera un rastro que configura un perfil altamente descriptivo de la personalidad de su titular.

Derecho a la Autodeterminación Informativa

Derecho paralelo de nueva generación consistente en el poder de cada ciudadano de decidir **quién tiene derecho a conocer sus datos personales**. No actúa en solitario, sino conjuntamente con el derecho al entorno digital, de modo que la vulneración de uno suele acarrear la del otro, con el consiguiente plus de lesividad.



No confundir estos dos derechos de nueva generación entre sí ni con el clásico derecho a la intimidad del **art. 18.1 CE**.

El Perfil Digital como Objeto de Protección

Un dato aislado puede parecer irrelevante: una búsqueda en Google, una compra en línea, un «like» en una red social. Sin embargo, la suma de todos ellos produce lo que el Tribunal Supremo denomina un **«perfil altamente descriptivo de la personalidad»** del investigado, que puede revelar ideologías, creencias religiosas, aficiones, información sanitaria u orientación sexual.

Datos sensibles expuestos

- Ideologías y creencias religiosas
- Información sobre la salud
- Orientación sexual
- Aficiones e intereses personales

Fuentes de generación

- Navegación por Internet
- Redes sociales y foros
- Comercio electrónico
- Mensajería y correo electrónico

Consecuencia jurídica

La intromisión injustificada en este entorno equivale, en terminología del TS, a **«desnudar virtualmente a una persona»**. De ahí la protección reforzada que impone la [LO 13/2015](#).

Distinción Fundamental: Entorno Virtual vs. Secreto de las Comunicaciones

Uno de los errores más frecuentes en examen consiste en confundir estos dos derechos. El Tribunal Supremo ha trazado una nítida línea divisoria con consecuencias procesales de primer orden, pues el régimen de autorización judicial difiere sustancialmente.

Derecho al Entorno Virtual

Comunicaciones concluidas, cerradas, bloqueadas. Se integra en el derecho a la intimidad informática ([art. 18.1 CE](#)). La información existe en el dispositivo por un proceso técnico de conservación. La Policía Judicial puede actuar **en caso de urgencia sin autorización judicial previa**, pero comunicándolo al Juez en el plazo máximo de [24 horas](#), que dispondrá de [72 horas](#) para ratificar o revocar ([art. 588 sexies c 4 LECrim](#)).

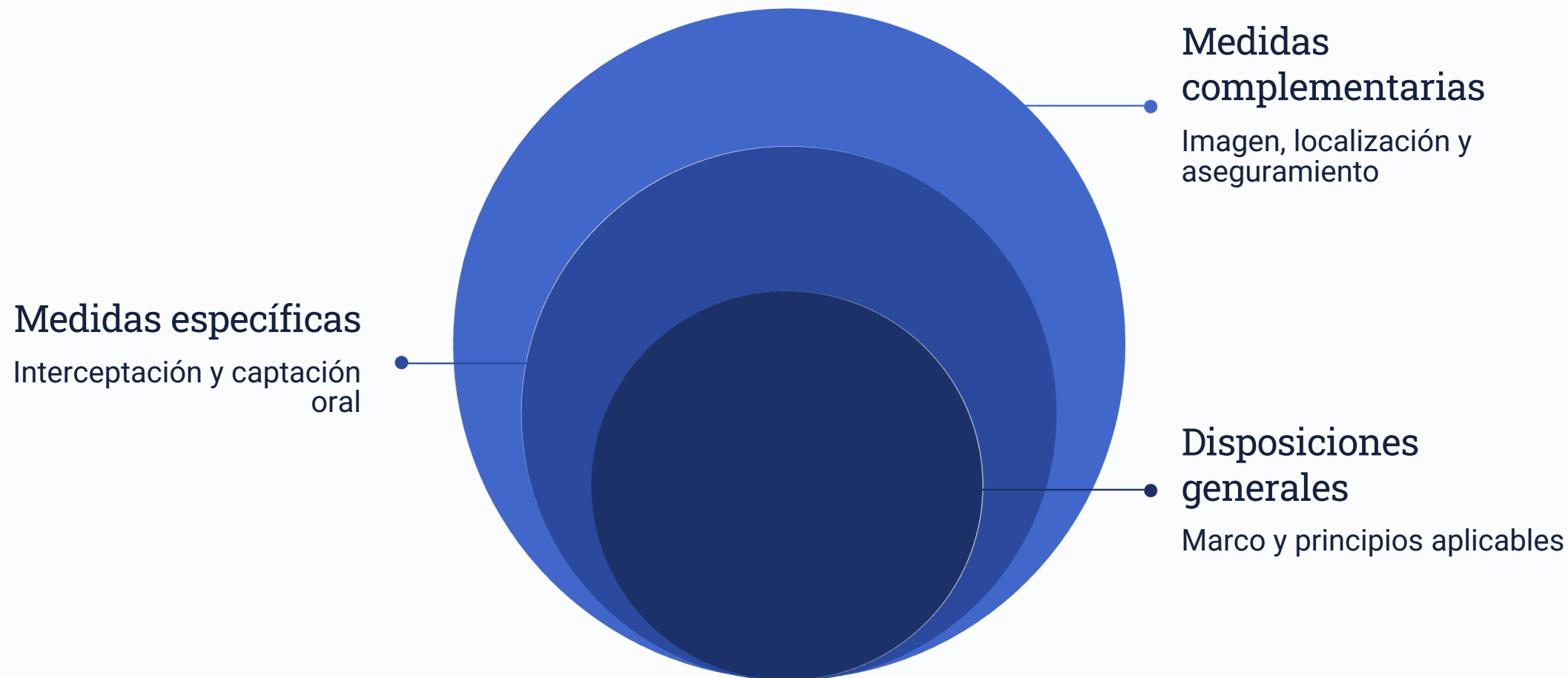
Secreto de las Comunicaciones

Comunicaciones vivas, en curso, en tránsito. Protegido por el [art. 18.3 CE](#). Requiere **siempre y sin excepción autorización judicial previa y expresa**. La ausencia de dicha autorización contamina irreversiblemente la prueba obtenida y determina su nulidad.

- 📄 Ejemplo práctico de examen: el acceso policial a la agenda de contactos de un móvil incautado afecta al derecho a la **intimidad** (no al secreto de las comunicaciones), pues los datos están cerrados y no fluyen en tiempo real. Por ello puede practicarse, con carácter urgente, sin autorización judicial previa.

II. Las Medidas de Investigación Tecnológica: Disposiciones Generales

La [LO 13/2015, de 5 de octubre](#), introdujo en el Título VIII del Libro II de la LECrim un régimen completo de medidas de investigación tecnológica, articuladas en torno a un Capítulo IV de disposiciones comunes y capítulos específicos para cada medida. Todas ellas —con la única excepción de la captación de imagen en lugares públicos— **precisan autorización judicial expresa**.



Los Seis Principios Rectores de las Medidas Tecnológicas

El [art. 588 bis a 1 LECrim](#) enumera los principios que vertebran toda medida de investigación tecnológica. Son de cumplimiento acumulativo y su inobservancia acarrea la nulidad de la diligencia.



1. Legalidad

Toda medida debe estar **expresamente prevista en la LECrim**. Sin ley previa, escrita, cierta y vigente no cabe adoptar ninguna medida de investigación tecnológica. No hay margen para la oportunidad judicial.



2. Especialidad

La medida debe estar estrechamente vinculada a la **investigación de un delito concreto** y en curso. No cabe adoptar medidas preventivas, cautelares apriorísticas o de vigilancia abstracta.



3. Idoneidad

La medida seleccionada debe ser **adecuada y útil** para los fines de la investigación, tanto en su ámbito objetivo, subjetivo como temporal. Delimita quiénes pueden ser investigados, por qué delitos y durante cuánto tiempo.



4. Excepcionalidad

Solo procede cuando **no existen medidas menos gravosas igualmente útiles** para el esclarecimiento. Se prioriza siempre la medida más efectiva y menos lesiva de los derechos fundamentales ([art. 588 bis a 4 LECrim](#)).



5. Necesidad

La medida es **imprescindible** porque sin ella la investigación no puede avanzar ni obtenerse información que permita aproximarse al conocimiento del hecho delictivo y la identidad de su autor.



6. Proporcionalidad

El sacrificio de derechos fundamentales no puede ser superior al beneficio público obtenido. El Juez pondera gravedad del hecho, trascendencia social, intensidad de los indicios y relevancia del resultado ([art. 588 bis a 5 LECrim](#)).

El Procedimiento de Autorización Judicial

Las medidas de investigación tecnológica solo pueden solicitarse por el **Ministerio Fiscal o la Policía Judicial** —nunca por la acusación particular o popular—. La solicitud se tramita en **pieza separada y secreta** sin necesidad de declarar expresamente el secreto de la causa.

Requisitos de la solicitud —

- Descripción del hecho e identidad del investigado
- Razones detalladas que justifican la medida e indicios de criminalidad
- Datos de identificación del investigado y medios empleados
- Extensión y contenido de la medida
- Unidad investigadora de la Policía Judicial
- Forma de ejecución y duración solicitada
- Sujeto obligado a colaborar, si es conocido

Contenido del Auto habilitante — art. 588 bis c LECrim

- Hecho punible y calificación jurídica con indicios racionales
- Identidad de los investigados y afectados
- Extensión de la medida y motivación sobre sus principios rectores
- Unidad investigadora designada
- Duración y periodicidad de la información al Juez
- Finalidad perseguida
- Sujeto obligado a colaborar y deber de secreto bajo apercibimiento de desobediencia

Plazo para resolver: 24 horas desde la presentación de la solicitud.

Hallazgos Espontáneos y Cesación de la Medida

Descubrimientos Casuales

Las informaciones obtenidas durante la ejecución de una medida tecnológica que revelen la existencia de hechos delictivos distintos de los investigados —denominados «**hallazgos espontáneos**» o «**descubrimientos casuales**»— pueden trasvasarse a la investigación de esos nuevos hechos, siempre que el nuevo Juez o Jueza competente autorice inmediatamente su incorporación a ese procedimiento foráneo.

Cesación y Prórrogas

Las medidas tecnológicas **no pueden exceder del tiempo imprescindible** para el esclarecimiento de los hechos. Pueden prorrogarse mediante auto motivado mientras subsistan las causas que las motivaron. Transcurrido el plazo sin prórroga, cesa la medida a todos los efectos. Cada medida tiene su propio plazo máximo —que estudiaremos en cada epígrafe específico—.

- ❏ Error de examen frecuente: confundir la duración de la intervención de comunicaciones (3 meses, prorrogables hasta 18 meses) con la del registro remoto (1 mes, hasta 3 meses) o la del seguimiento y localización (3 meses, hasta 18 meses).



EPÍGRAFE III

III. La Interceptación de las Comunicaciones Telefónicas y Telemáticas

La interceptación de las comunicaciones telefónicas y telemáticas constituye la medida de investigación tecnológica de mayor potencial invasivo y, al mismo tiempo, de mayor utilidad en la investigación de delitos graves. Consiste en la interceptación de todos aquellos dispositivos que permiten la comunicación telefónica o telemática, tanto del presunto autor del hecho delictivo como de los terceros que se relacionan con él.

Ámbito Objetivo: ¿Para Qué Delitos se Autoriza?

El ámbito objetivo de la interceptación **no es ilimitado**. La LECrim lo circunscribe a cuatro bloques de delitos, que justifican el sacrificio del derecho a la intimidad ([art. 18.1 CE](#)) y al secreto de las comunicaciones ([art. 18.3 CE](#)):

Bloque 1

Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión ([art. 579.1 LECrim](#)).

Bloque 2

Delitos cometidos en el seno de un **grupo u organización criminal** ([art. 579.1 LECrim](#)).

Bloque 3

Delitos de **terrorismo** ([art. 579.1 LECrim](#)).

Bloque 4

Delitos cometidos **a través de instrumentos informáticos** o cualquier tecnología de la información o la comunicación ([art. 588 ter a LECrim](#)).

La razón de ser de esta restricción es clara: la extraordinaria lesividad de la medida aconseja que no se convierta en un instrumento de uso indiscriminado, abusivo o cotidiano. La propia Ley fija los primeros límites por razón de la gravedad o naturaleza de los delitos.

Ámbito Subjetivo, Extensión y Régimen de Autorización

¿A quién puede interceptarse?

- Terminales usados por el investigado de forma habitual u ocasional (art. 588 ter b 1)
- Terminales de titularidad del investigado o de cuyo mero uso se sirva (art. 588 ter b 2 I)
- Los de la **víctima** cuando sea previsible un grave riesgo para su vida o integridad (art. 588 ter b 2 II)
- Los de **terceros** si el investigado se sirve de ellos para transmitir o recibir información, o si el titular colabora con el investigado en sus fines ilícitos (art. 588 ter c)

Extensión de la medida

- Registro y grabación del contenido de la comunicación
- Conocimiento del origen o destino en tiempo real
- Localización geográfica del origen o destino
- Datos de tráfico asociados o de valor añadido

Duración — art. 588 ter g LECrim

Duración inicial: **3 meses**, prorrogables por períodos sucesivos de igual duración hasta un máximo de **18 meses**.

❏ Excepción al requisito de autorización judicial previa: en caso de urgencia por terrorismo o bandas armadas, puede ordenarla el **Ministro del Interior o el Secretario de Estado de Seguridad**, comunicándolo al Juez en **24 horas**; el Juez ratifica o revoca en **72 horas** (art. 588 ter d 3 LECrim).

Deber de Colaboración y Régimen de las Grabaciones

Deber de colaboración —

Todos los prestadores de servicios de telecomunicaciones, de acceso a redes o de la sociedad de la información están obligados a prestar asistencia al Juez, al MF y a los agentes de la Policía Judicial designados. El incumplimiento puede constituir **delito de desobediencia**. También pesa sobre ellos un deber de guardar secreto acerca de las actividades requeridas.

Régimen de las grabaciones — art. 588 ter f y i LECrim

La Policía Judicial pone a disposición del Juez, con la periodicidad fijada, la transcripción de los pasajes de interés y las grabaciones íntegras. Se garantiza la autenticidad e integridad mediante **sellado o firma electrónica avanzada**. Alzado el secreto, se entregan a las partes copia de las grabaciones y transcripciones, salvo los datos referentes a la vida íntima no relacionados con los hechos investigados.



EPÍGRAFE IV

IV. La Captación y Grabación de Comunicaciones Orales Mediante Dispositivos Electrónicos

Esta medida consiste en la adquisición, percepción o grabación del sonido —y, en su caso, de la imagen— durante las conversaciones directas que mantenga el investigado, pudiendo practicarse tanto en la vía pública como en espacios cerrados o en el propio domicilio. A diferencia de la interceptación de comunicaciones, aquí las conversaciones son directas, orales, lanzadas al aire, sin soporte técnico de canal cerrado.

Notas Características y Derechos Fundamentales Afectados

Notas definitorias

- Puede limitarse al sonido o extenderse a la imagen, siempre que el Juez lo autorice **expresamente** en la misma resolución
- Puede practicarse en la vía pública, en lugar cerrado o en el domicilio
- En caso de entrada domiciliaria, la resolución habilitante debe extender su motivación a la procedencia del acceso a esos espacios íntimos
- Los dispositivos pueden colocarse en el exterior o interior del domicilio
- Solo puede autorizarse para **encuentros concretos y previsibles**, nunca de forma indiscriminada

Derechos fundamentales sacrificados

Art. 18.1 CE

Intimidad personal

Art. 18.1 in fine CE

Propia imagen (si se graba imagen)

Art. 18.2 CE

Inviolabilidad domiciliaria (si opera en domicilio)

Art. 18.3 CE

Secreto de las comunicaciones

Presupuestos de Validez y Ámbito Objetivo – art. 588 quater b LECrim

El Legislador ha establecido unos exigentes presupuestos de validez que el Juez debe verificar antes de autorizar esta medida de singular agresividad.

1 Constreñimiento a encuentros concretos y previsibles

La medida debe limitarse a diálogos que puedan tener lugar en **uno o varios encuentros concretos** del investigado con terceras personas, sobre cuya previsibilidad existan indicios. Nunca puede autorizarse de forma indiscriminada o ilimitada respecto de toda la vida cotidiana del investigado. Los encuentros posteriores a la autorización requieren **nueva resolución judicial**.

2 Ámbito objetivo restringido

Solo procede para la investigación de: (1) delitos dolosos con pena máxima de al menos **3 años de prisión**; (2) delitos cometidos en el seno de grupos u organizaciones criminales; y (3) delitos de terrorismo. A diferencia de la interceptación de comunicaciones, **no incluye los delitos tecnológicos genéricos**.

3 Previsibilidad de obtener datos esenciales

Debe poder racionalmente preverse que los dispositivos aportarán **datos esenciales y de relevancia probatoria** para el esclarecimiento de los hechos y la identificación del autor. El mero recurso a la medida sin esta perspectiva de utilidad la invalida.

❏ Contenido mínimo de la autorización judicial: además de los extremos generales del [art. 588 bis c](#), debe constar mención concreta al **lugar o dependencias** y a los **específicos encuentros** sometidos a vigilancia ([art. 588 quater b LECrim](#)).



EPÍGRAFE V

V. La Utilización de Dispositivos Técnicos de Captación de la Imagen, Seguimiento y Localización

El Capítulo VII del Título VIII del Libro II de la LECrim regula conjuntamente dos medidas de investigación tecnológica que, pese a sus aparentes similitudes, presentan presupuestos de validez radicalmente distintos: la captación de imagen en lugares públicos **no precisa autorización judicial**, mientras que el seguimiento y localización **sí la precisa**.

Captación de Imagen en Lugares Públicos

¿En qué consiste?

Obtención y grabación, efectuada por la Policía Judicial, a través de cualquier medio técnico, de la persona investigada cuando se encuentre en un **lugar o espacio público**, para facilitar su identificación, localizar los instrumentos o efectos del delito, u obtener datos relevantes para el esclarecimiento de los hechos. Puede extenderse a personas distintas del investigado cuando su exclusión reduciría relevantemente la utilidad de la vigilancia o existan indicios de su relación con el investigado ().

¿Por qué no precisa autorización judicial?

La escasa lesividad de esta medida —que se practica siempre en un espacio público, donde los ciudadanos quedan expuestos a la vista de terceros, fuera del entorno protector del domicilio— justifica que la LECrim no exija autorización judicial previa. La Policía Judicial puede actuar «**de propia autoridad**», sin perjuicio de que la imagen sea un derecho fundamental ciertamente afectado ([art. 18.1 CE](#)).



Requisito inexcusable: solo puede practicarse frente a una persona determinada respecto de la cual exista una investigación en curso. No cabe la vigilancia indiscriminada.

Seguimiento y Localización Mediante Dispositivos Técnicos

Esta segunda medida consiste en la persecución y ubicación del investigado durante un período de tiempo relativamente dilatado mediante la utilización de dispositivos como **radiotransmisores, balizas de seguimiento, ondas GPS o drones**. El grado de afectación del derecho a la intimidad ([art. 18 CE](#)) es lo suficientemente alto como para exigir autorización judicial expresa.

Autorización judicial previa (regla general)

El Juez o Jueza autorizará caso por caso, previa concurrencia de razones de necesidad, idoneidad y proporcionalidad, con especificación del concreto medio técnico a utilizar.

Excepción: urgencia — [art. 588 quinquies b 4 LECrim](#)

Si el retraso frustraría la investigación, la Policía Judicial puede colocar el dispositivo sin autorización previa, dando cuenta a la autoridad judicial en el plazo máximo de [24 horas](#). El Juez ratifica o acuerda el cese inmediato en ese mismo plazo. Si acuerda el cese, la información obtenida **carece de efectos en el proceso**.

Duración — [art. 588 quinquies c LECrim](#)

Máximo de [3 meses](#) desde la autorización. Excepcionalmente, prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de [18 meses](#), si los resultados lo justifican.

Deber de colaboración — [art. 588 quinquies b 3 LECrim](#)

Los prestadores, agentes y colaboradores deben prestar asistencia al Juez, al MF y a los agentes de Policía Judicial, bajo apercibimiento de incurrir en **delito de desobediencia**.



EPÍGRAFE VI

VI. El Registro de Dispositivos de Almacenamiento Masivo de Información

Esta medida consiste en la extracción de información relevante para la investigación incorporada a toda clase de dispositivos de almacenamiento masivo: ordenadores fijos y portátiles, teléfonos móviles, tabletas, pen drives, memorias externas, disquetes, CDs, USBs e incluso nubes y repositorios digitales. Su importancia radica en que estos dispositivos pueden albergar simultáneamente datos protegidos por distintos derechos fundamentales.

La Doble Modalidad: Dentro y Fuera del Domicilio

La LECrim distingue dos regímenes según el lugar de incautación del dispositivo, reforzando así la idea de que la autorización judicial para la **entrada y registro físicos** no se extiende automáticamente al **registro electrónico**.



REGISTRO EN DOMICILIO:
Requiere autorización judicial previa y expresa para el acceso al contenido electrónico (art. 588 sexies a LECrim). La simple incautación no legitima el acceso.



REGISTRO FUERA DEL DOMICILIO:
Los agentes informan al Tribunal de la incautación; si es indispensable se autoriza el acceso. En urgencia, la Policía Judicial examina y el Juez ratifica (arts. 588 sexies b, c 4 LECrim).

Garantías Específicas del Registro Electrónico

Contenido de la resolución habilitante

El auto del Tribunal de instancia que autoriza el acceso al contenido de los dispositivos debe fijar:

- Los términos y el alcance del registro
- La posibilidad de realizar copias de los datos informáticos
- Las condiciones para asegurar la **integridad de los datos**
- Las garantías de preservación que permitan, en su caso, un dictamen pericial

Deber de colaboración — art. 588 sexies c LECrim

Las autoridades pueden ordenar a cualquier persona que conozca el funcionamiento del sistema o las medidas de protección de los datos que facilite la información necesaria (por ejemplo, contraseñas o passwords), salvo que derive en una carga desproporcionada, bajo apercibimiento de incurrir en **delito de desobediencia**.

Quedan eximidos: personas dispensadas de declarar por razón de parentesco y las que no pueden declarar en virtud del secreto profesional.

📄 Diferencia clave para el examen: el **registro de dispositivos** (Epígrafe VI) supone entrada física + registro electrónico. El **registro remoto** (Epígrafe VII) es exclusivamente electrónico, sin ningún acceso físico. No confundirlos.

VII. El Registro Remoto sobre Equipos Informáticos

El registro remoto sobre equipos informáticos es la medida de investigación tecnológica de mayor agresividad sobre el derecho fundamental a la intimidad virtual. Consiste en la entrada y registro **exclusivamente electrónico**, a distancia y sin conocimiento del investigado, mediante la implantación de un software informático — coloquialmente conocido como «**troyano**»— en el equipo informático o dispositivo electrónico del investigado.



Régimen Jurídico del Registro Remoto

1

Catálogo de delitos — [art. 588 septies a 1 LECrim](#)

1) Organizaciones criminales; 2) Terrorismo; 3) Delitos contra menores o personas con discapacidad; 4) Delitos contra la Constitución, traición y defensa nacional; 5) Delitos cometidos a través de instrumentos informáticos o tecnología TIC.

2

Contenido de la resolución — [art. 588 septies a 2 LECrim](#)

Dispositivos objeto de la medida; alcance y forma de acceso; agentes autorizados; posibilidad de copias; medidas de preservación de la integridad de los datos.

3

Duración

Máximo de [1 mes](#), prorrogable por iguales períodos hasta un máximo de [3 meses](#).
Plazo sensiblemente inferior al de la interceptación de comunicaciones, reflejo de la mayor agresividad de la medida.

Si los agentes comprueban que los datos buscados están en otro sistema informático, lo comunicarán al Juez, quien podrá autorizar una **ampliación de los términos del registro**. El deber de colaboración ([art. 588 septies b 2 LECrim](#)) incluye la obligación de guardar secreto sobre las actividades requeridas, con la misma estructura de exenciones que en el registro de dispositivos.

VIII. La Orden de Conservación de Datos Archivados

Naturaleza y función

El MF o la Policía Judicial pueden requerir a cualquier persona física o jurídica la **conservación y protección** de datos o informaciones concretas incluidas en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión. Es una medida cautelar de aseguramiento probatorio que evita la destrucción de datos mientras se tramita la autorización judicial de acceso.

Plazo — art. 588 octies LECrim

Los datos se conservarán durante un período máximo de **noventa días**, prorrogable **una sola vez** hasta que se autorice la cesión o se cumplan **ciento ochenta días**.

- ❏ Esta medida no es una medida de investigación propiamente dicha, sino una medida de aseguramiento previo a la obtención de los datos. No permite acceder al contenido, solo conservarlo.

Cuadro Comparativo: Las Medidas de Investigación Tecnológica

Medida	Autorización judicial	Ámbito objetivo	Duración máxima	Art. LECrim
Interceptación comunicaciones telefónicas/telemáticas	Siempre (excepción: terrorismo, Ministro Interior)	+3 años, organización criminal, terrorismo, delitos TIC	3 meses / hasta 18 meses	588 ter a ss.
Captación y grabación de comunicaciones orales	Siempre, previa y expresa	+3 años, organización criminal, terrorismo	Por encuentros autorizados	588 quater a ss.
Captación de imagen en lugar público	NO precisa	Sin restricción objetiva	Sin límite fijo	588 quinquies a
Seguimiento y localización	Sí (urgencia: 24h posterior)	Sin restricción objetiva expresa	3 meses / hasta 18 meses	588 quinquies b/c
Registro de dispositivos almacenamiento	Sí (urgencia: 24h, ratificación 72h)	Sin restricción objetiva expresa	La que fije el auto	588 sexies a ss.
Registro remoto («troyano»)	Siempre, previa y expresa	Organizaciones criminales, terrorismo, menores, Constitución, TIC	1 mes / hasta 3 meses	588 septies a ss.
Conservación de datos archivados	Posterior (para cesión)	Sin restricción objetiva	90 días / hasta 180 días	588 octies

CASOS PRÁCTICOS – Corrección Razonada

A continuación se desarrolla la corrección de los seis casos prácticos de la Lección 16, siguiendo el criterio metodológico establecido: prevalencia de los apuntes sobre la ley, que actúa como complemento normativo. Se utilizan los marcadores visuales indicados en las instrucciones de corrección.

Caso I

Intimidad informática y derecho al entorno virtual

Caso II

Disposiciones generales de las medidas tecnológicas

Caso III

Interceptación de comunicaciones telefónicas y telemáticas

Caso IV

Captación y grabación de comunicaciones orales

Caso V

Captación de imagen, seguimiento y localización

Caso VI

Registro de dispositivos de almacenamiento masivo

Caso I: Intimidad Informática y Derecho al Entorno Virtual

Planteamiento y cuestiones

El supuesto de hecho, articulado sobre la célebre cita de O.W. Holmes en el caso Olmstead (1928) y sobre doctrina del TS español, plantea el debate entre la obtención de la verdad material y el respeto irrenunciable a los derechos fundamentales durante la investigación penal.

● Cuestión a) ¿Existe un derecho a la intimidad informática?

Correcto y completo. Sí existe. El TS ha proclamado el «**derecho al entorno digital**» como derecho de nueva generación, que protege la ingente cantidad de datos que se acumulan en ordenadores y dispositivos electrónicos. Su vulneración equivale, en terminología del TS, a «desnudar virtualmente a una persona». Se vincula además al paralelo **derecho a la autodeterminación informativa**. ● Referencia normativa: [LO 13/2015](#).

● Cuestión b) ¿Cuándo se entiende resentido el derecho a la intimidad virtual?

Correcto. Se entiende resentido cuando se produce una **intromisión en el espacio digital** de las personas ante la sospecha de una actuación delictiva concluida, en curso o en vías de comisión. No obstante, la injerencia estará justificada si concurren los parámetros de legalidad, jurisdiccionalidad, especialidad, necesidad, idoneidad y proporcionalidad ([art. 588 bis a 1 LECrim](#)).

● Cuestión c) ¿Qué datos integran el derecho al entorno virtual?

Correcto. Toda la información generada voluntaria o involuntariamente por el usuario: navegación, redes sociales, descargas, comercio electrónico, grupos de noticias. Los datos individualmente considerados pueden parecer irrelevantes, pero en su conjunto configuran un perfil altamente descriptivo de la personalidad que merece protección constitucional reforzada.

● Cuestión d) Diferencia entre entorno virtual y secreto de las comunicaciones

Correcto, aunque debe precisarse: el entorno virtual protege datos bloqueados, comunicaciones concluidas. El secreto de las comunicaciones ([art. 18.3 CE](#)) protege las comunicaciones en curso, vivas, en tránsito. **Consecuencia procesal capital:** la intromisión en el secreto de las comunicaciones requiere siempre autorización judicial previa; la intromisión en el derecho a la intimidad virtual admite, en urgencia, actuación policial sin autorización previa ([art. 588 sexies c 4 LECrim](#)).

● Cuestión e) «El fin no justifica los medios»

Correcto. La verdad material **no puede obtenerse a cualquier precio**. Solo es legítima cuando se alcanza dentro de las exigencias del ordenamiento jurídico. Las medidas tecnológicas lesionan no solo la intimidad, sino también la imagen, el secreto de las comunicaciones e incluso la inviolabilidad domiciliaria. De ahí que su correcta adopción, seguimiento y valoración precisen una **tutela reforzada** de Jueces y Magistrados. El «Gobierno no puede ponerse al nivel del delincuente» (Holmes, Olmstead, 1928).

✔ ● **Conclusión clave:** La respuesta al Caso I es globalmente correcta. No se detectan errores sustanciales. El alumno demuestra dominio de la distinción entre los dos derechos de nueva generación y de la doctrina del TS sobre la verdad material formalizada.

Caso II: Las Nuevas Medidas de Investigación Tecnológica – Disposiciones Generales

Planteamiento

El supuesto plantea la necesidad de una **específica autorización judicial** para acceder al contenido de los dispositivos electrónicos, incluso cuando existe una previa decisión judicial que autorizó el acceso al lugar donde se encontraban. Se subraya la justificación del tratamiento unitario de los datos contenidos en ordenadores y teléfonos móviles ([art. 588 sexies a y b LECrim](#)).

● Cuestión a) Diferencia en la autorización: secreto de comunicaciones vs. intimidad

Correcto. La diferencia es esencial y de consecuencias procesales determinantes: la intromisión en el **secreto de las comunicaciones** requiere siempre autorización judicial previa y expresa —sin ninguna excepción posible—, por imperativo del [art. 18.3 CE](#). La intromisión en el **derecho a la intimidad** en el entorno virtual admite, en caso de urgencia, actuación policial sin dicha autorización previa, comunicándola al Juez en el plazo máximo de **24 horas** y debiendo el Juez ratificar o revocar en **72 horas** ([art. 588 sexies c 4 LECrim](#)).

● Cuestión b) ¿Todas las medidas precisan autorización judicial previa?

Correcto, con matiz importante. La regla general es la autorización judicial previa. La **única excepción absoluta** es la captación de imagen en lugares o espacios públicos, que no precisa autorización judicial en ningún caso ([art. 588 quinquies a LECrim](#)). Las demás admiten excepcionalmente actuación policial urgente a posteriori (seguimiento/localización, registro de dispositivos) o por el Ministro del Interior (interceptación de comunicaciones en casos de terrorismo).

● Cuestión c) Principios de legalidad y especialidad

Correcto. *Legalidad:* toda medida debe estar **expresamente prevista en la LECrim**, sin margen para la oportunidad. *Especialidad:* la medida debe vincularse a la **investigación de un delito concreto y en curso**. No caben medidas preventivas ni de vigilancia abstracta. El principio de especialidad impide la existencia de un «Estado espía».

● Cuestión d) Idoneidad, excepcionalidad, necesidad y proporcionalidad

Correcto. *Idoneidad:* la medida es adecuada para el ámbito objetivo, subjetivo y temporal de la investigación. *Excepcionalidad:* solo procede cuando no existe otra medida menos gravosa igualmente útil. *Necesidad:* la investigación no puede avanzar sin la medida. *Proporcionalidad:* el sacrificio de derechos no es superior al beneficio público; el Juez pondera gravedad del hecho, trascendencia social, intensidad de indicios y relevancia del resultado ([art. 588 bis a 5 LECrim](#)).

● Cuestión e) Carácter subsidiario del consentimiento

Correcto. La autorización judicial es **subsidiaria del consentimiento** del titular del dispositivo: si el afectado accede libremente a la inspección, no es necesaria resolución judicial alguna. La necesidad de autorización judicial opera, pues, únicamente cuando no existe ese consentimiento libre e informado del investigado.

✓ ● **Conclusión:** Respuesta del Caso II globalmente correcta. Se recomienda precisar que el principio de proporcionalidad judicial tiene un **margen escaso** porque la LECrim ya ha realizado la ponderación legislativa al fijar los delitos susceptibles de investigación tecnológica.

Caso III: Interceptación de las Comunicaciones Telefónicas y Telemáticas

Planteamiento

El supuesto parte de las características del *smartphone* como instrumento híbrido que permite simultáneamente comunicaciones en curso y almacenamiento de comunicaciones concluidas. Ello obliga a distinguir qué régimen protector se aplica a cada tipo de información, con especial relevancia en la práctica forense.

● Cuestión a) ¿En qué consiste exactamente la interceptación?

Correcto. Consiste en la interceptación de todos aquellos dispositivos que permiten la comunicación telefónica o telemática —en sus distintas modalidades: conversación oral, SMS, email, WhatsApp, Telegram, etc.— tanto del presunto autor como de los terceros que se relacionan con él, con las extensiones subjetivas y de contenido previstas en los [arts. 588 ter b al 588 ter m LECrim](#).

● Cuestión b) ¿El ámbito objetivo es ilimitado?

Correcto. No. Se restringe a los cuatro bloques de delitos ya estudiados. La razón de ser de esta restricción es su extraordinaria lesividad en los derechos fundamentales del [art. 18.1 y 18.3 CE](#): la medida no puede devenir habitual, sistemática ni indiscriminada.

● Cuestión c) Excepción a la autorización judicial previa

Correcto. La única excepción es la prevista en el [art. 588 ter d 3 LECrim](#): en caso de urgencia por bandas armadas o terrorismo, puede ordenarla el **Ministro del Interior** o, en su defecto, el **Secretario de Estado de Seguridad**, comunicándolo al Juez en [24 horas](#) y debiendo el Juez ratificar o revocar en [72 horas](#). La racionalidad de la excepción descansa en la urgencia de la persecución del terrorismo y en la coordinación entre las Administraciones encargadas de la seguridad del Estado.

● Cuestión d) Deber de colaboración

Correcto. Los prestadores de servicios de telecomunicaciones, de acceso a red y de la sociedad de la información deben prestar al Juez, al MF y a la Policía Judicial la asistencia y colaboración precisas ([art. 588 ter e LECrim](#)). También deben guardar **secreto** sobre las actividades requeridas. El incumplimiento puede integrar **delito de desobediencia**.

● Cuestión e) Actos «relativamente restrictivos» vs. «radicalmente restrictivos»

Importante matización que falta en la respuesta tipo: los actos «relativamente restrictivos» afectan a derechos fundamentales de menor intensidad de protección constitucional (intimidad, imagen, datos personales) y admiten en principio intervención policial sin autorización judicial previa. Los «radicalmente restrictivos» afectan al secreto de las comunicaciones ([art. 18.3 CE](#)) o a la inviolabilidad domiciliaria ([art. 18.2 CE](#)) y requieren **siempre y sin excepción** autorización judicial. Los actos en el ámbito electrónico se ubican, según el caso, en ambas categorías: el acceso a comunicaciones en curso es radicalmente restrictivo; el acceso al entorno virtual (datos bloqueados) puede ser relativamente restrictivo con la válvula de urgencia del [art. 588 sexies c 4 LECrim](#).



● **Conclusión:** El Caso III está bien resuelto en sus líneas generales. El punto más importante que debe añadirse es la distinción entre actos relativamente y radicalmente restrictivos y su aplicación diferenciada a los actos de investigación electrónicos.

Caso IV: Captación y Grabación de Comunicaciones Orales

Planteamiento

El supuesto subraya que la captación y grabación de comunicaciones orales en el domicilio del investigado supone una injerencia cualitativamente superior a la del resto de medidas tecnológicas, pues penetra en el «núcleo duro» de la intimidad personal y familiar. El TS advierte que asimilarla a otras medidas del [art. 18 CE](#) distorsionaría los términos de su legitimidad.

● Cuestión a) Singularidades propias respecto del conjunto de medidas

Correcto y bien argumentado. La expectativa de privacidad de quien cierra la puerta de su domicilio no es comparable a la de quien usa un teléfono o un vehículo con baliza GPS. La medida no solo afecta al investigado sino también a su familia, residentes habituales y visitantes esporádicos. El grado de motivación de la resolución, el respeto a la proporcionalidad y la duración deben ser **escrupulosamente valorados** judicialmente ([art. 588 quater a LECrim](#)).

● Cuestión b) Diferencia con la interceptación de comunicaciones

Correcto. La captación oral opera en sede física (lugar abierto o cerrado), con conversaciones directas y orales. La interceptación opera en sede electrónica —canal telefónico o telemático—. Ambas precisan medios tecnológicos para grabar las conversaciones, pero el origen de las conversaciones es radicalmente distinto: físico y oral en un caso, electrónico y mediado en el otro.

● Cuestión c) Derechos fundamentales sacrificados

Correcto. Intimidad personal ([art. 18.1 CE](#)); propia imagen si se graba imagen ([art. 18.1 in fine CE](#)); secreto de las comunicaciones ([art. 18.3 CE](#)); inviolabilidad domiciliar si opera en el domicilio ([art. 18.2 CE](#)). Se trata de la medida con mayor número de derechos fundamentales simultáneamente sacrificados.

● Cuestión d) Contenido mínimo de la autorización judicial

Correcto. Además de los extremos generales del [art. 588 bis c LECrim](#), el auto debe contener: mención concreta al **lugar o dependencias** y a los **específicos encuentros** sometidos a vigilancia. Si la medida se practica en el domicilio, la resolución debe extender su motivación a la procedencia del acceso a esos espacios. La autorización de imagen debe ser **expresa** en la misma resolución.

● Cuestión e) ¿Ámbito objetivo ilimitado o restringido?

Correcto. El ámbito objetivo está **restringido**: delitos dolosos con pena de al menos 3 años, organización criminal y terrorismo. A diferencia de la interceptación de comunicaciones, no incluye los delitos tecnológicos genéricos. La opción legislativa es conveniente: la mayor agresividad de la medida justifica un ámbito objetivo más reducido que el de la interceptación de comunicaciones, que sí incluye los delitos TIC.

✔ ● **Conclusión:** Caso IV muy bien resuelto. Ningún error sustancial. Se recomienda destacar expresamente que la resolución que autoriza la grabación en domicilio debe **motivar específicamente** la procedencia de la entrada y no simplemente extenderse de forma automática desde otro acto de investigación previo.

Caso V: Dispositivos de Captación de Imagen, Seguimiento y Localización

Planteamiento

El supuesto describe una investigación en la que se utilizaron balizas de seguimiento en dos vehículos (A y B) con múltiples defectos procedimentales: cambio de baliza a mitad de la investigación, ausencia de justificación de los indicios, falta de plazo en el auto originario (subsano al día siguiente), y ausencia del informe de geolocalización en tiempo real respecto del vehículo B.

● Cuestión a) ¿En qué consiste la captación de imagen?

Correcto. Consiste en la obtención y grabación por la Policía Judicial de la imagen del investigado en **lugar o espacio público**, para facilitar su identificación, localizar efectos del delito u obtener datos relevantes. No requiere autorización judicial previa ([art. 588 quinquies a LECrim](#)). Puede extenderse a personas distintas del investigado con los requisitos legales.

● Cuestión b) ¿En qué consiste el seguimiento y localización?

Correcto. Persecución y ubicación del investigado durante un período dilatado mediante dispositivos como radiotransmisores, balizas de seguimiento, GPS o drones. A diferencia de la captación de imagen, supone una vigilancia continua que afecta intensamente al derecho a la intimidad ([art. 18 CE](#)), razón por la que sí precisa autorización judicial.

● Cuestión c) ¿Cuál no precisa autorización judicial y por qué?

Correcto. La **captación de imagen en lugares públicos** no precisa autorización judicial, por su escasa lesividad: los ciudadanos están expuestos a la vista de terceros fuera del ámbito domiciliario. La vigilancia permanente mediante seguimiento y localización sí precisa autorización, por su mayor intensidad invasiva.

● Cuestión d) Excepción a la autorización previa del seguimiento

Correcto. En casos de urgencia donde el retraso frustraría la investigación, la Policía Judicial puede colocar el dispositivo y dar cuenta a la autoridad judicial en el plazo máximo de **24 horas** ([art. 588 quinquies b 4 LECrim](#)). El Juez ratifica o acuerda el cese inmediato. Si acuerda el cese, la información obtenida **carece de todo efecto en el proceso**.

● Cuestión e) Distinto nivel de protección: ámbito privado vs. público

Correcto. La intimidad se desarrolla en ambos ámbitos, pero la mayor fuerza invasiva en el ámbito privado —desarrollada generalmente en el domicilio— merece una protección legal reforzada. En el espacio público, los ciudadanos mantienen formalidades sociales que reducen razonablemente sus expectativas de privacidad absoluta.

⚠️ ● Observación crítica sobre el supuesto: los defectos procedimentales descritos en el caso (falta de plazo, ausencia de justificación de los indicios, ausencia del informe de geolocalización en tiempo real respecto del vehículo B) son **determinantes de la nulidad** de la medida respecto del vehículo B y, cuando menos, de la anulabilidad del auto originario respecto del vehículo A por falta de plazo. El alumno debe identificar y señalar expresamente estas consecuencias.

● Caso VI: El Registro de Dispositivos de Almacenamiento Masivo

● Planteamiento

El supuesto justifica el tratamiento unitario de los datos contenidos en dispositivos de almacenamiento masivo a partir del **derecho al entorno digital**, proclamando que el acceso policial a esos contenidos no puede legitimarse por un acto unilateral de las Fuerzas de Seguridad sino que requiere **autorización judicial** como verdadero presupuesto habilitante de naturaleza formal.

● Cuestión a) ¿En qué consiste el registro de dispositivos de almacenamiento masivo?

Correcto. Consiste en la extracción de información incorporada a ordenadores, teléfonos móviles, tabletas, pen drives, memorias externas, USBs, nubes y repositorios digitales. Su rasgo esencial es la **plurifuncionalidad de los datos** que alberga: datos técnicos, comunicaciones concluidas, fotografías, datos de geolocalización, correos electrónicos descargados, etc., con distintos regímenes constitucionales de protección.

● Cuestión b) ¿La autorización de entrada y registro domiciliario se extiende automáticamente al electrónico?

No, y este es el punto más importante del caso. La autorización judicial para la entrada y registro físicos **no comporta la extensión automática** al registro electrónico de los dispositivos hallados en el domicilio. El registro electrónico precisa una extensión expresa y específica en la misma resolución judicial, debidamente motivada ([art. 588 sexies a LECrim](#)): «La simple incautación de cualquiera de estos dispositivos, practicada durante el transcurso de la diligencia de registro domiciliario, **no legitima el acceso a su contenido**».

● Cuestión c) Diferencia entre registro de dispositivos y registro remoto

Correcto. El registro de dispositivos implica una **entrada física** previa en el lugar donde se encuentran los dispositivos + registro electrónico posterior. El registro remoto es exclusivamente electrónico, **sin ningún acceso físico**, mediante la implantación de un software («troyano») en el equipo del investigado a distancia y sin su conocimiento.

● Cuestión d) ¿Existe diferencia según sea dentro o fuera del domicilio?

Correcto. *Dentro del domicilio:* la autorización judicial debe extenderse expresamente al registro electrónico en el mismo auto que autoriza la entrada y registro físicos. *Fuera del domicilio:* los agentes comunican la incautación al Tribunal, quien decide si autoriza el acceso; en urgencia, la Policía puede examinar directamente el contenido comunicándolo en **24 horas** y el Juez ratifica o revoca en **72 horas** ([art. 588 sexies b y c 4 LECrim](#)).

● Cuestión e) Distinto nivel de salvaguarda constitucional

Correcto. Los dispositivos de almacenamiento masivo coexisten con datos de distinto rango constitucional: comunicaciones protegidas por el [art. 18.3 CE](#) (máximo nivel), datos personales e íntimos ([art. 18.1 CE](#)) y datos de geolocalización y personales ([art. 18.4 CE](#)). La LECrim ha optado por un tratamiento unitario reforzado que exige autorización judicial previa como **presupuesto habilitante formal**, actuando con carácter anticipado en todo caso.

✓ ● **Conclusión:** Caso VI. El punto medular —la no extensión automática de la autorización de entrada domiciliaria al registro electrónico— está correctamente identificado y argumentado. Se recomienda precisar la triple proyección constitucional de los datos albergados en los dispositivos.

Resumen de Conclusiones Clave — Errores Típicos de Examen

✗ Error 1

Confundir «entorno virtual» (datos bloqueados, intimidad) con «secreto de las comunicaciones» (comunicaciones en curso). Son dos derechos distintos con regímenes de autorización radicalmente diferentes.

✗ Error 2

Creer que todas las medidas tecnológicas precisan autorización judicial. La **captación de imagen en lugares públicos** es la única excepción absoluta.

✗ Error 3

Confundir los plazos: interceptación de comunicaciones (3 meses / hasta 18 meses) ≠ registro remoto (1 mes / hasta 3 meses) ≠ conservación de datos (90 días / hasta 180 días).

✗ Error 4

Creer que la autorización de entrada y registro domiciliario permite automáticamente el registro de los dispositivos electrónicos hallados en el domicilio. Requiere autorización **expresa adicional** (art. 588 sexies a LECrim).

✗ Error 5

Olvidar que el ámbito objetivo de la captación y grabación de comunicaciones orales **no incluye los delitos tecnológicos**, a diferencia de la interceptación de comunicaciones que sí los incluye (art. 588 ter a LECrim).

✗ Error 6

Confundir el «registro de dispositivos» (entrada física + registro electrónico) con el «registro remoto» (exclusivamente electrónico, mediante troyano, sin contacto físico).

Conclusión General

«No se puede obtener la verdad real a cualquier precio. Solo aquello que es compatible con la defensa del elemento nuclear de los derechos fundamentales, dentro de los parámetros fijados en la Ley.» – Tribunal Supremo

Marco normativo esencial

- [LO 13/2015, de 5 de octubre](#) – Reforma de la LECrim en materia de medidas de investigación tecnológica
- [Arts. 18.1, 18.2, 18.3 y 18.4 CE](#) – Derechos fundamentales afectados
- [Arts. 588 bis a al 588 octies LECrim](#) – Régimen completo de las medidas tecnológicas

La lección más importante

Las medidas de investigación tecnológica representan el mayor sacrificio admisible de los derechos fundamentales en el proceso penal. Su legitimidad depende del cumplimiento acumulativo y riguroso de todos los principios rectores: legalidad, especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. El fin – descubrir al delincuente – nunca justifica prescindir de estos principios.

Nota de uso y advertencia del documento

 **Advertencia importante:** Este documento se ofrece sin ánimo de lucro a los estudiantes matriculados y con finalidad exclusivamente informativa y de apoyo al estudio. Su contenido ha sido elaborado a partir de textos legales y manuales procesales especializados.

El documento refleja la normativa vigente en la fecha de su elaboración, no constituye un texto oficial y no sustituye al material recomendado por el equipo docente. En consecuencia, pueden existir inexactitudes o modificaciones normativas posteriores que no se encuentren recogidas en el mismo.

Para un adecuado estudio de la oposición, se recomienda la consulta directa de los textos legales oficiales vigentes, así como el material recomendado por el equipo docente.

 **Propiedad intelectual:** Queda prohibida la reproducción total o parcial de este documento, incluido el escaneo o soporte digital, su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros métodos), sin el permiso previo y por escrito del autor. La infracción puede ser constitutiva de delito contra la propiedad intelectual (**art. 270 y siguientes del Código Penal**).



Fundamentos
— Jurídicos —