

1. Según el artículo 1 apartado 3º de la LO 1/82, de 5 de mayo, el derecho al honor, a la intimidad personal y familiar y a la propia imagen es:

- a) Irrenunciable, inalienable e imprescindible.
- b) Irrenunciable, inalienables y prescriptible.
- c) Irrenunciable, inalienable e imprescriptible.



2. Según la LO 1/82 sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, ¿qué tendrá consideración de intromisión ilegítima?

- a) El emplazamiento en lugar privado de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.
- b) La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.
- c) La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.

3. Una de las características de la prueba digital es:

- a) Su tangibilidad.
- b) Su volatilidad.
- c) Ambas son correctas.



4. La autorización judicial para admitir la utilización de dispositivos técnico de seguimiento, ¿en qué deberá basarse para la valoración del interés público en la ponderación del principio de proporcionalidad?

- a) 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.
- b) 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, así como las capacidades económicas y sociales del individuo.
- c) En la gravedad del hecho, su trascendencia económica o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

5. Según la Ley de Enjuiciamiento Criminal, en aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse una medida de investigación cuando:

- a) Cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho.
- b) Cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea dificultada sin el recurso a esta medida.
- c) Ambas respuestas son correctas.

6. ¿Quién puede acordar o solicitar las medidas reguladas en el Capítulo IV del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal?

- a) El juez, de oficio
- b) El Ministerio Fiscal o la Policía judicial, a instancia de parte
- c) Ambas respuestas son correctas.



7. ¿Cuál de las tres opciones de respuesta no corresponde con uno de los presupuestos para autorizar la interceptación de las comunicaciones telefónicas y telemáticas?

- a) Que se trate de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información.
- b) Que se trate de delitos cometidos en el seno de un grupo u organización criminal.
- c) Que se trate de delitos dolosos o imprudentes castigados con pena con límite máximo de, al menos 3 años de prisión.

8. Para poder interceptar las comunicaciones de un investigado, los terminales o medios de comunicación objeto de intervención deben ser:

- a) Aquellos que el investigado utilice habitual u ocasionalmente.
- b) Aquellos que el investigado utilice de manera habitual.
- c) Aquellos que el investigado utilice ocasionalmente.

9. ¿Podrán ser intervenidos los terminales o medios de comunicación de la víctima?

- a) Sí, siempre que sea necesario y proporcional a las circunstancias.
- b) Sí, siempre que sea sin su conocimiento y peligre gravemente su vida.
- c) Sí, solo cuando sea previsible un grave riesgo para su vida o integridad.



10. ¿Cuál será la duración máxima inicial de la interceptación de terminales o medios de comunicación?

- a) De tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de doce meses.
- b) De seis meses, prorrogables por períodos sucesivos de igual o inferior duración hasta el plazo máximo de doce meses.
- c) De tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

11. ¿En qué **casos de urgencia** puede ordenar el **Ministro del Interior**, o en su defecto el **SES**, la **interceptación de las comunicaciones**?

- a) En casos de urgencia en los que el delito esté relacionado con la actuación de bandas armadas o elementos terroristas y, existan motivos racionales para realizar la intervención.
- b) En casos de urgencia en los que el delito esté relacionado con la actuación de bandas armadas o elementos terroristas y, existan razones fundadas que hagan imprescindible la medida.
- c) El Ministerio del Interior y el SES no puede ordenar la interceptación de las comunicaciones telefónicas y telemáticas, ya que es competencia exclusiva del juez competente.

12. En el caso de que los **agentes de Policía Judicial** necesiten **identificar y localizar el equipo o dispositivo de conectividad y los datos de identificación del usuario mediante un número IP**:

- a) Estos podrán solicitar directamente a los agentes sujetos al deber de colaboración la cesión de los datos que permitan tales pesquisas.
- b) Estos solicitarán del Juez de Instrucción que requiera de los agentes sujetos al deber de colaboración la cesión de los datos que permitan tales pesquisas.
- c) Estos podrán solicitar a través del Juez de Instrucción o, directamente a los agentes sujetos al deber de colaboración, la cesión de los datos que permitan tales pesquisas.

13. ¿Es necesaria **autorización judicial** para que la **Policía Judicial** realice la **identificación de los terminales mediante captación de códigos de identificación de aparatos o sus componentes**?

- a) Sí, ya que el Juez de Instrucción es el único competente para poder autorizar tales intervenciones.
- b) No, ya que basta con la autorización del Ministro del Interior o, en su defecto, del SES.
- c) No, los agentes podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación.

14. ¿Puede obtenerse la **escucha y grabación de las conversaciones privadas que se puedan obtener junto a las imágenes del investigado**?

- a) Sí, siempre que se trate de grabaciones en un lugar público y con autorización judicial.
- b) Sí, cuando expresamente lo autorice la resolución judicial que acuerde la medida.
- c) No, a menos que se trate de conversaciones en un lugar público, para lo que no es necesario autorización judicial.

15. Cuando la **Policía Judicial** deba poner a **disposición judicial las comunicaciones grabadas lo hará**:

- a) Mediante el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de un informe.
- b) Mediante el soporte original o copia de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones que considere de interés.
- c) Mediante el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones que considere de interés.

16. ¿Puede la **Policía Judicial** captar **imágenes de la persona investigada si ello fuera necesario para facilitar su identificación**?

- a) Sí, tanto en lugares públicos como privados, podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada.
- b) Sí, cuando la persona investigada se encuentre en lugar o espacio público.
- c) Sí, cuando la persona investigada se encuentre en lugar o espacio privado.

17. ¿Puede un **agente de la Policía Judicial** acceder al **ordenador incautado del investigado durante la práctica de un registro domiciliario**?

- a) Solo si obtiene una autorización del juez competente.
- b) Sí, la orden de registro domiciliario incluye per se la posible aprehensión y acceso a los dispositivos necesarios.
- c) No, ya que esta actuación no corresponde realizarla en el propio domicilio.

18. ¿Cuándo podrá ser **autorizado el registro remoto de un equipo informático**?

- a) Cuando el delito cometido sea contra menores o personas con capacidad modificada judicialmente.
- b) Cuando se trate de delitos contra la Constitución, de traición y relativos a la defensa nacional.
- c) A y B son correctas.

19. ¿Qué **no deberá especificar la resolución judicial que autorice un registro remoto**?

- a) La autorización, en su caso, para la realización y conservación de copias electrónicas auténticas de los datos informáticos.
- b) Los agentes autorizados para la ejecución de la medida.
- c) 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.

20. ¿Para qué está **facultado el agente encubierto informático**?

- a) Para intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos, así como para obtener imágenes y grabaciones de conversaciones de los encuentros previstos entre el agente y el investigado, aún cuando se desarrollen en el interior de un domicilio.
- b) Para intercambiar o enviar por sí mismo archivos lícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.
- c) Para intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos, cuando cuente con autorización específica para ello.



33. **El descubrimiento y revelación de secretos, en general, se castiga con el Código Penal español en:**
 a) El artículo 197. b) Los artículos 264 y siguientes. c) Los artículos 278 y 279.
34. **La adquisición ilícita de una contraseña que permita acceder a una parte de un sistema informático lo pena el Código Penal español en su artículo:**
 a) 264 bits. b) 264. c) 264 ter.
35. **¿Qué artículo, de los siguientes, recoge el delito de pornografía infantil en nuestro Código Penal vigente?:**
 a) El artículo 187. b) El 189. c) El 197.
36. **¿Qué oración no se corresponde con el contenido de algunas de las frases que conforma el lema de los ciberactivistas del grupo Anonymous?:**
 a) El conocimiento es libre. b) La venganza es nuestra arma. c) No perdonamos. No olvidamos.
37. **En general, la técnica de suplantación de identidad en Internet por medio de falsificación de DNS, IP, etc. se conoce con el término:**
 a) Carding. b) Hoax. c) Spoofing.
38. **¿Qué es un "keylogger" ?**
 a) Un sistema de suplantación de identidad en Internet.
 b) Software que registra las combinaciones de teclas.
 c) Suplantación de servidores DNS.
39. **¿Qué circunstancia se requiere para que los delitos de calumnias e injurias cometidos a través de Internet puedan considerarse como delitos informáticos?**
 a) Que se hagan con publicidad manifiesta.
 b) Que sean de carácter muy grave.
 c) Que este sistema sea determinante para la consecución del delito.
40. **Señala la respuesta que contenga un principio no considerado básico en la Ley de Protección de Datos:**
 a) Información y finalidad.
 b) Abundancia, calidad y consentimiento.
 c) Seguridad, consentimiento y finalidad.
41. **La guías telefónicas, respecto al tratamiento de datos personales, tienen la siguiente catalogación:**
 a) Fichero de contenido reservado.
 b) Fuente accesible al público.
 c) Fichero de datos personales de carácter semiprivado.
42. **Tanto los ficheros establecidos para la investigación del terrorismo y delincuencia organizada, como los que tienen datos especialmente protegidos:**
 a) Se regulan por sendas leyes específicas para cada una de estas materias.
 b) Debe ser comunicada su existencia a la Agencia de Protección de Datos.
 c) Les son de aplicación por completo la LOPD.
43. **El derecho que tiene una persona cuyos datos estén almacenados en un fichero a que la Agencia de Protección de Datos le muestre los que tiene almacenados en el Registro de Protección de Datos, se conoce como:**
 a) Derecho de acceso.
 b) Derecho de consulta.
 c) El Registro de Protección de Datos no tiene ficheros de datos personales.
44. **Los datos personales que hagan referencia al origen racial, la salud, y la vida sexual:**
 a) Solo pueden ser recabados si, por razones de interés general, así lo disponga una ley.
 b) Tienen que ser autorizados por su titular, pero no tiene por que haber una ley que así lo disponga.
 c) Estos datos no necesitan más trámite que el resto de datos personales que se puedan recoger en un fichero.
45. **¿Qué naturaleza tiene la Agencia de Protección de Datos?:**
 a) Entidad pública de derecho privado, con personalidad jurídica derivada de la administración del Estado.
 b) Ente de derecho público, con personalidad jurídica propia, que actúa con plena independencia de las Administraciones públicas.
 c) Órgano de derecho público dependiente de la Administración del Estado, de quien deriva su personalidad jurídica.
46. **Se necesita autorización o mandamiento judicial para:**
 a) La investigación de una conversación en un foro abierto de Internet.
 b) La intervención de una comunicación realizada por medio de un correo electrónico.
 c) Ambas respuestas son correctas.
47. **¿Qué tipo de medios generadores de datos tienen la obligación de guardar los operadores de telecomunicaciones?:**
 a) Los procedentes de teléfonos fijos, móviles y acceso a Internet.
 b) Los procedentes de teléfonos fijos, móviles y acceso a Internet y correo electrónico.
 c) Los procedentes de teléfonos fijos, móviles y acceso a Internet y correo electrónico y telefonía VoIP.
48. **¿Es necesaria la autorización judicial para localizar transmisiones entre ordenadores, siguiendo la tecnología conocida como P2P?**
 a) No es necesaria en ningún caso, ya que el servidor se limita a poner a disposición de todo ordenador que lo solicite un determinado fichero.
 b) Sí es necesaria, ya que la transmisión de datos entre dos ficheros es privada.
 c) Es necesaria la autorización judicial para acceder a los datos generados por las transmisiones, pero no para el rastreo de transmisiones potencialmente delictivas.

