CONSEJO GENERAL DEL PODER JUDICIAL
ESCUELA JUDICIAL

PLAN ESTATAL 2017

La nueva regulación de la LECRIM en materia de investigación tecnológica.

Madrid, año 2017

Conclusiones

COORDINADOR

D. José Manuel SANCHEZ SISCART

Presidente de la Audiencia Provincial de Soria

RELATORA

D.ª Yolanda RUEDA SORIANO

Magistrada de la Sección Nº 21 de la Audiencia Provincial de Barcelona

53 CUESTIONES SOBRE LA NUEVA REGULACIÓN DE LA LECRIM EN MATERIA DE INVESTIGACIÓN TECNOLÓGICA

Contenido

A) INTRODUCCIÓN. 6

B) DEBATE SOBRE CUESTIONES GENERALES, PRINCIPIOS RECTORES, DEBER DE COLABORACIÓN Y MEDIDAS DE ASEGURAMIENTO. 6

1. Con anterioridad a la reforma de la Lecrim operada por la LO 13/2015, la jurisprudencia admitía la motivación del auto autorizando intervenciones telefónicas, por remisión al oficio policial (ejemplo STS 676/2012). Tras la reforma, ¿sigue siendo admisible la motivación por remisión? 6

2. ¿Es necesario conocer el titular de la línea a intervenir? ¿Cabe acordar intervenciones telefónicas para la identificación de sospechosos? 8

3. ¿Cabe intervenir las comunicaciones telefónicas de los familiares de un sospechoso para su localización? ¿de sus abogados? 9

4. ¿Cabe acordar intervenciones telefónicas para la averiguación de paradero de un condenado en fase de ejecución de sentencia? 10

5. ¿Cabe acordar la intervención de los terminales de terceros que estén siendo utilizados maliciosamente sin su conocimiento? 11

6. ¿Qué criterios deben manejarse a la hora de determinar la extensión de la medida? ¿cómo debe motivarse? ¿se puede autorizar sin distinción la intervención de las comunicaciones y de todos sus datos asociados? 11

7. ¿Se pueden distinguir diferentes niveles de protección según se trate de datos de contenido, tráfico o de usuarios? ¿qué valores constitucionales se ven afectados en cada caso? ¿cuáles son las consecuencias de su respectiva protección constitucional? ¿Se transforma el régimen de garantías según haya finalizado o no el proceso comunicativo? 13

8. A diferencia del Ministerio Fiscal, ¿puede solicitar una intervención telefónica el resto de acusaciones? ¿Cómo se gestionaría el secreto en ese caso? 18

9. En relación con la notificación a terceros ¿qué debe entenderse por imposibilidad, esfuerzo desproporcionado, o perjuicio para futuras investigaciones? 19

10. ¿A quién alcanza el deber de colaboración de los prestadores de servicios previsto en el art. 588 ter e? ¿Cuál es el alcance y la extensión del deber de colaboración contemplado en el artículo 588 septies b)? ¿Podrían oponerse? ¿Cómo? ¿en qué casos? 19

11. Si los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, se niegan a facilitar a la policía judicial los datos de titularidad de un número de teléfono o de cualquier otro medio de comunicación o los datos identificativos de cualquier medio de comunicación, ¿Deben ordenarlos los Jueces cuándo la ley no lo exige? 21

12. ¿Alcanza el deber de colaboración a las entidades públicas o privadas que se encuentran ubicadas en el extranjero? 22

13. ¿Cómo debe procederse en caso de "hallazgo casual"? 22

14. ¿En qué se basa la doctrina del "silencio estratégico"? ¿Cabe entenderla superada a la vista de la actual regulación? 26

15. ¿Se puede adoptar cualquier medida de investigación tecnológica, previa solicitud policial que se remite a fuentes confidenciales para motivar la base indiciaria? 28

16. ¿Cómo debe interpretarse el art. 588 ter i en lo relativo a la entrega de grabaciones a las partes? 30

17. ¿Cabe reconocer expectativa razonable de privacidad en grupos de chat con numerosos componentes? ¿Cómo podemos delimitar lo público y lo privado? 31

18. ¿En qué supuestos es aplicable el plazo de 5 años para la conservación y destrucción de copias? ¿Qué finalidad cumple este plazo? ¿En qué supuestos cabría acordar excepcionalmente la conservación de las copias más allá de este plazo? ¿Qué garantías adicionales deberían establecerse? 33

19. ¿Por qué debe llevarse a cabo el borrado y eliminado de estos datos?¿Quién debe ordenarlo? 35

20. Ante el silencio de la ley al respecto, ¿Cuál sería el régimen de impugnación por las defensas de las transcripciones de las conversaciones telefónicas grabadas o del volcado de los datos contenidos en un ordenador, USB, móvil…? 36

21. ¿Encuentra amparo constitucional la regulación contenida en los artículos 588 ter d), 588 quinties b) y 588 sexies c), que permite a la Policía Judicial establecer medidas de vigilancia en casos de urgencia? 38

22. Si la medida adoptada por la Policía Judicial es posteriormente revocada por el Juez/a, ¿Qué sucede con la información obtenida? ¿Debe comunicarse a la persona afectada? 40

C) DEBATE SOBRE INTERVENCIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS; GRABACIÓN COMUNICACIONES ORALES, CAPTACIÓN DE IMÁGENES; DISPOSITIVOS DE SEGUIMIENTO Y LOCALIZACIÓN. 41

23. ¿Cabe grabar comunicaciones orales de sospechosos con abogados? ¿en encuentros sexuales? ¿en aseos o lavabos? etc. 41

24. ¿Cabe instalar escuchas orales en el domicilio de un tercero no investigado? 43

25. ¿Puede la Policía motu propio auxiliar a un particular para grabar la conversación de un tercero? 44

26. ¿Se pueden colocar y utilizar dispositivos electrónicos de escucha y grabación en una celda? 44

27. ¿Cabe instalar aparatos de escucha en un domicilio consintiendo el acceso el comorador en caso de contraposición de intereses con el investigado? 45

28. ¿Cabe instalar aparatos de escucha en un domicilio tras franquear el acceso el morador pero sin su conocimiento? 47

29. ¿Qué valor probatorio cabe reconocer a las imágenes con cámara oculta en dependencias privadas, consultas profesionales, vía pública, etc.? 47

30. ¿Qué salvaguardas deben establecerse desde el prisma de la proporcionalidad? 49

31. ¿Cabe la observación mediante "drones" de espacios al aire libre dentro de propiedades particulares? 50

D) DEBATE SOBRE REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO; REGISTROS REMOTOS; AGENTE ENCUBIERTO ONLINE. 53

32. ¿Cabe acceder al registro de un dispositivo de almacenamiento masivo con el consentimiento del sujeto? 53

33. ¿Está obligado a proporcionar las claves de acceso o ceder la huella digital? 54

34. ¿Qué razones justifican la exigencia de autorización judicial en el registro de dispositivos de almacenamiento masivo? 54

35. ¿A qué se refiere la frase "interés constitucionalmente legítimo" que utiliza el art. 588 sexies c, apartado 4 para habilitar a la policía judicial el acceso al contenido de un ordenador, de un móvil, sin autorización judicial? 56

36. ¿Qué límites cabe establecer en el registro de dispositivos de almacenamiento masivo? 58

37. El letrado de la defensa comunica que en el ordenador del investigado se encuentra información enmarcada en la relación cliente-letrado que afecta al derecho de defensa, ¿cómo debemos proceder? 60

38. ¿Deben entenderse incluidos los datos relativos a las llamadas telefónicas u otras comunicaciones, si nada expresa la autorización judicial –art. 588 sexies c).4-? 64

39. ¿Cabe trasladar a la lectura de los correos electrónicos las mismas garantías respecto a la apertura de correspondencia privada? 66

40. ¿Cómo se lleva a cabo el volcado de estos datos? ¿Debe estar presente el Letrado de la Administración de Justicia? ¿Y el letrado de la defensa? ¿Qué medidas deben adoptarse para garantizar la autenticidad e integridad de los datos conservados? 67

41. ¿Habría que observar algún tipo de garantía especial en el caso de que los archivos se encuentren en la nube alojados en otro país? 69

42. ¿Pueden los padres acceder a los teléfonos móviles de sus hijos? 71

43. ¿Puede el empresario acceder a los equipos informáticos de la empresa asignados a un empleado? ¿Tiene el trabajador en este contexto expectativa de confidencialidad? 72

44. ¿Qué derechos pueden verse afectados en un registro remoto? ¿qué tipo de software puede ser utilizado? ¿qué tipo de límites o salvaguardas cabe establecer? 74

45. ¿Qué tipo de archivos podría intercambiar un agente encubierto online? 74

46. ¿Son susceptibles de manipulación las evidencias electrónicas? 75

E) DEBATE SOBRE INCORPORACIÓN AL PROCESO DE DATOS DE USUARIOS, TRÁFICO, Y CONTENIDO. AUXILIO JUDICIAL INTERNACIONAL. 77

47. ¿Cabe acceder a los datos de comunicaciones electrónicas conservados por los proveedores de servicios? ¿En qué casos? 77

48. ¿Cabe cesión de datos de comunicaciones electrónicas en relación con un delito imprudente –pe, accidente aéreo, ferroviario, tráfico- u otros delitos de menor gravedad? 80

49. ¿Qué datos conservados pueden facilitar los proveedores de servicios a los agentes policiales sin necesidad de autorización judicial? ¿Qué diferencias existen entre los artículos 588 ter j) –datos vinculados a procesos de comunicación- y 588 ter m) –datos de titularidad de teléfonos o medios de comunicación-? 85

50. ¿Qué problemática plantean los rastreos de direcciones de IP con ocasión de intercambios de archivos P2P en funciones de prevención de delitos? ¿Qué diferencias existen entre el art. 588 ter k –identificación y localización de direcciones IP por parte de la Policía Judicial- y el art. 588 ter m –averiguación de titularidades de un número de teléfono o medio de comunicación por la Policía Judicial? 86

51. ¿Puede la policía judicial captar mediante artificios técnicos el IMSI o el IMEI sin autorización judicial? ¿Cabe identificar déficit de salvaguardas en el art. 588 ter l? 87

52. ¿Cabe hablar de “intimidad compartida” en el ámbito de la pareja o familiar? ¿Qué problemática plantea la violencia de género cometida a través de medios tecnológicos (redes sociales, correo electrónico, SMS, etc)? 90

53. ¿Cabe reconocer valor probatorio a la información obtenida ilícitamente por un particular? 90

AUTORES:

Dª. Yolanda Rueda Soriano, cuestiones nº 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 15, 16, 19, 20, 21, 22, 23, 24, 26, 29, 32, 33, 36, 40, 42, 44, 50, 52, 53.

D. José Manuel Sánchez Siscart, cuestiones nº 7, 12, 13, 14, 17, 18, 25, 27, 28, 30, 31, 34, 35, 37, 38, 39, 41, 43, 45, 46, 47, 48, 49, 51.

A) INTRODUCCIÓN.

El desarrollo de nuevas tecnologías ha posibilitado la aparición de renovadas formas de delincuencia, a menudo transnacional y complejamente organizada. Afortunadamente también nos aporta eficaces vías de investigación, basadas principalmente en la averiguación de los flujos de información generados por los sistemas de comunicación o por otras formas de intrusión, antes desconocidas, en diversos espacios de privacidad o exclusión constitucionalmente protegidos.

La reforma procesal en esta materia, operada por LO 13/2015 de 5 de octubre, resultaba inaplazable. Junto a diversos principios rectores, plasmados ahora de forma expresa en el texto legal, la nueva normativa incorpora una extensa regulación de la interceptación de las comunicaciones telefónicas y telemáticas, utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, registro de dispositivos de almacenamiento masivo, registro remoto sobre equipos informáticos, agente encubierto informático, captación y grabación de comunicaciones orales, etc., que deben ser objeto de debate, sistematización, y detenido análisis.

Especial atención merece la cesión y conservación de datos de tráfico o usuarios, analizando la compleja relación entre la nueva normativa y la regulación contenida de la Ley 25/2007, a la luz de la STJUE de 8 de abril de 2014 y 21 de diciembre de 2016 y de otras cuestiones prejudiciales que aún penden ante dicho Tribunal, así como las soluciones a las que se ha llegado en otros países de la Unión Europea, que condicionan el ámbito de lo posible en el terreno de la asistencia judicial internacional.

En suma, en este seminario pretendemos profundizar en la nueva regulación de las medidas de investigación tecnológica, los diferentes niveles de protección constitucional en función de los diversos ámbitos de privacidad que pueden verse afectados, la potencialidad de las nuevas herramientas tecnológicas de investigación, en aras a reforzar la lucha experta y eficaz contra las nuevas formas de criminalidad y cibercrimen.

B) DEBATE SOBRE CUESTIONES GENERALES, PRINCIPIOS RECTORES, DEBER DE COLABORACIÓN Y MEDIDAS DE ASEGURAMIENTO.

Con anterioridad a la reforma de la Lecrim operada por la LO 13/2015, la jurisprudencia admitía la motivación del auto autorizando intervenciones telefónicas, por remisión al oficio policial (ejemplo STS 676/2012). Tras la reforma, ¿sigue siendo admisible la motivación por remisión?

Por motivación por remisión –o per relationem- se entienden los supuestos en los que la resolución judicial que autoriza una medida injerente en algún derecho fundamental –generalmente interviniendo conversaciones telefónicas- no contiene los indicios tenidos en cuenta para su adopción, aunque los elementos indiciarios existentes aparecen de forma suficiente, ya en el oficio policial que la precede o, en su caso, en otras resoluciones dictadas en la misma causa, a las que se remite el auto judicial autorizante (STS 523/2017). Se ha justificado su admisión alegándose que si bien el requisito de la motivación constituye una exigencia inexcusable, se reconoce que en el momento inicial del procedimiento en el que ordinariamente se acuerda la intervención telefónica, no resulta exigible una justificación fáctica exhaustiva, pues se trata de una medida adoptada, precisamente, para profundizar en una investigación no acabada, por lo que únicamente pueden conocerse unos iniciales elementos indiciarios (STS 533/2017). Es por ello por lo que el Tribunal Constitucional ha considerado suficiente que la motivación fáctica de este tipo de resoluciones se fundamente en la remisión a los correspondientes antecedentes obrantes en las actuaciones y concretamente a los elementos fácticos que consten en la correspondiente solicitud policial, o en el informe o dictamen del Ministerio Fiscal, cuando se ha solicitado y emitido.

Se reconoce que no es una técnica jurisdiccional modélica sino que deja mucho que desear, ya que la autorización judicial debería ser autosuficiente. Pero no obstante, la doctrina constitucional admite que la resolución judicial pueda considerarse suficientemente motivada si, integrada con la solicitud policial, a la que se remite, o con el informe o dictamen del Ministerio Fiscal en el que solicita la intervención contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad, resultando en ocasiones redundante que el Juzgado se dedique a copiar y reproducir literalmente la totalidad de lo narrado extensamente en el oficio o dictamen policial que obra unido a las mismas actuaciones, siendo más coherente que extraiga del mismo los indicios especialmente relevantes (STC 72/2010). Es decir, que la remisión al oficio policial no por poco escrupulosa, deja de satisfacer la exigencia constitucional, trasladándose la cuestión al examen de ese oficio policial para determinar si logra dar cumplimiento a las exigencias materiales que demanda el principio de proporcionalidad (STS 495/205). La resolución judicial debe comprobar por tanto la presencia de indicios suficientes, es decir, que aunque haya remisión, el/la juez/a debe valorar la suficiencia de los indicios para alcanzar la probabilidad que justifica las sospechas, ya que esta labor de valorar la suficiencia de los indicios es una valoración que no puede hurtarse al/a juez/a instructor/a y no puede descansar exclusivamente en el criterio o juicio de los agentes policiales. (STS 495/2015 ya citada). Lo contrario sería inadmisible ya que no cabría hablar de remisión sino de simple yuxtaposición a modo de una suerte de estampillado de la comunicación policial (STS 101/2017).

Con la reforma operada por LO 13/2015, de 5 de octubre, el artículo 588 bis c) detalla el contenido mínimo que debe tener el auto judicial autorizando la medida de investigación de que se trate, exigiendo *la concreción del hecho punible objeto de*

investigación y su calificación jurídica, así *como expresará los indicios racionales en los que funde la medida.*

No hubo unanimidad en el seminario en cuanto a si esta exigencia es o no incompatible con la motivación por remisión a la que nos hemos referido. Un grupo consideramos que el contenido reglado y exigido del auto judicial impide operar por reenvío al oficio policial debido a que la resolución debe contener necesariamente tanto la base fáctica como la expresión de los indicios que sustentan la adopción de la medida. Y ello porque el precepto referido expresa el contenido mínimo del auto "*la resolución judicial que autorice la medida concretará al menos los siguientes extremos"*. De hecho, esa parece ser la intención del legislador como explica la Exposición de Motivos de la LO 13/2017, al decir que *la reforma ha considerado adecuado no abandonar los aspectos formales de la solicitud y del contenido de la resolución judicial habilitante. La práctica forense no es ajena a casos de solicitudes policiales y de ulteriores resoluciones judiciales que adolecen de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación. A evitar ese efecto se orienta la minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial que, en su caso, habilite la medida de injerencia.*

Por el contrario, otro grupo considera que a pesar de la nueva regulación, tiene cabida la remisión por motivación si contiene todos los elementos necesarios para considerar satisfechas las exigencias para llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva.

¿Es necesario conocer el titular de la línea a intervenir? ¿Cabe acordar intervenciones telefónicas para la identificación de sospechosos?

Hay unanimidad en considerar que no es necesario conocer al titular de la línea a intervenir. Ya el artículo 588 bis c) 3 contempla la posibilidad de ignorarse la identidad de la persona investigada al referir que la resolución judicial que autorice la medida concretará al menos los siguientes extremos: *b) la identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.*

En coherencia con el artículo 588 bis b) que regula el contenido de la petición de la medida de investigación tecnológica realizada por la policía judicial o el Ministerio Fiscal, y que debe identificar al investigado o cualquier otro afectado por la medida, *siempre que tales datos resulten conocidos,* 588 bis b) 2º. Se ha recogido así, como en muchos otros aspectos, la doctrina jurisprudencial creada en torno a una materia tan lacónicamente regulada. Así, la STS 73/2016, remitiéndose a sentencias anteriores -STS 48/2013, 877/2014- ya establecía que "*en cuanto a la intervención telefónica, en momento en el que su titular aún no es identificado, no supone una extralimitación en la injerencia; pues en autos, es la persona que en cada caso usa ese móvil, la persona*

que se desea investigar y sobre la que se aportan indicios de su actividad delictiva, al margen de cuál fuere su concreto nombre".

Es decir, que el hecho de que no se aporten otros datos de identidad no puede ser un obstáculo para la legitimidad de la interceptación. Pero es que incluso se ha admitido la validez de la medida en supuestos de falta de identificación, no ya del titular, sino incluso del usuario del terminal que luego resulta ser interceptado (STC 150/2006). Y su fundamento se encontraba en las dificultades que para la identificación de los titulares y usuarios de los teléfonos suponían los avances tecnológicos en el ámbito de la telefonía con la aparición de los teléfonos móviles y de las tarjetas prepago, en la investigación de delitos graves especialmente cuando se cometan en el seno de estructuras delictivas organizadas. Por lo que la previa identificación de los titulares o usuarios de las líneas telefónicas a intervenir no es imprescindible para entender expresado el alcance subjetivo de la medida.

Y en esta línea, el artículo 588 ter b-1º (en el ámbito ya de la regulación específica de las comunicaciones telefónicas y telemáticas) dispone que *los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado, debiendo ser completado por el 588 ter c.1) que dice que podrá acordarse la intervención judicial de las telecomunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información.* Por lo que interesa más el uso o la potencialidad de uso del terminal o del dispositivo que la relación de titularidad. Incluso la jurisprudencia del Tribunal Supremo ha resuelto supuestos de incorrecta identificación original en el oficio policial de los titulares y usuarios de los terminales telefónicos, resolviéndose que la previa identificación de los titulares o usuarios de las líneas telefónicas a intervenir no es imprescindible para entender expresado el alcance subjetivo de la medida, ya que son perfectamente legítimas aquéllas intervenciones telefónicas que recaen sobre sospechosos y se orientan a su identificación. Careciendo, por tanto, de relevancia constitucional el error respecto a la identidad de los titulares o usuarios de las líneas intervenidas.

Lógicamente, en estos casos en los que se interviene un terminal o dispositivo sin conocerse la identidad de su titular o para identificar a la persona sospechosa, al poderse afectar a un tercero, se exigirá una mayor motivación o una motivación reforzada.

¿Cabe intervenir las comunicaciones telefónicas de los familiares de un sospechoso para su localización? ¿de sus abogados?

En esta cuestión no ha habido unanimidad. Un grupo sostiene que sí cabe la intervención de las comunicaciones telefónicas de los familiares de un sospechoso para su localización y otro grupo niega dicha posibilidad.

En las disposiciones comunes a todas las medidas de investigación tecnológica establecidas en los artículos 588 bis a) a 588 bis k), concretamente en el 588 bis h) se permite la afectación de terceras personas por estas medida de investigación, remitiéndose en cuanto a los casos ya concretos y condiciones para ello a las disposiciones específicas en cada una de ellas. Y el artículo 588 bis a) 4-b, establece que solo podrá acordarse las medidas *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 gravemente dificultada sin el recurso a esta medida.* Sin embargo, de todas las medidas reguladas a continuación –interceptación de las comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, registro de dispositivos de almacenamiento masivo de información y registros remotos sobre equipos informáticos- solamente en dos de ellas se regula expresamente la posible afectación de terceros. En el ámbito de las intervenciones telefónicas y telemáticas y en el ámbito de la captación de la imagen, de seguimiento y de localización.

En el ámbito de las intervenciones telefónicas y telemáticas, los artículos 588 ter b) y c) permiten la afectación por la medida de un tercero, que no sea por tanto el investigado en los siguientes supuestos:

1. El terminal de la víctima cuando sea previsible un grave riesgo para su vida o integridad, (588 ter b) 2
2. El de un tercero cuando haya constancia de que la persona investigada lo utiliza para transmitir o recibir información, (588 ter c-1º).
3. El del tercero que se beneficia del delito o colabore con la persona investigada en sus fines ilícitos (588 ter c- 2º).

Por lo que de la interpretación del 588 bis a) 4-b) y del 588 ter c-), solamente se admitiría intervenir teléfonos de familiares para averiguar el paradero del sospechoso siempre que haya constancia de que este último utiliza el terminal del familiar para transmitir o recibir información, o cuando el familiar-titular del terminal o del medio de comunicación telemática colabore en los fines ilícitos o se beneficie de dicha actividad.

No obstante, en el seminario concluimos que se ha de hacer el necesario juicio de proporcionalidad en cada caso y que tampoco se puede excluir de entrada.

En cuanto a la intervención telefónica del abogado nos remitimos a la pregunta 24).

¿Cabe acordar intervenciones telefónicas para la averiguación de paradero de un condenado en fase de ejecución de sentencia?

Esta cuestión viene motivada por habérsela planteado algunos Juzgados de Instrucción, al permitirse en otros países de Derecho comparado.

La respuesta negativa es unánime ya que la adopción de alguna de las medidas reguladas en el Capítulo IV de la Lecrim introducido por LO 13/2015, solamente cabe en el marco de la instrucción, como así delimita el artículo 588 bis a) "*Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo…,* y en relación a la investigación de un delito concreto. Como ya se ha dicho, únicamente sería posible acordarla para averiguar el paradero del sospechoso (588 bis a-4 b), pero siempre en el marco de la investigación.

¿Cabe acordar la intervención de los terminales de terceros que estén siendo utilizados maliciosamente sin su conocimiento?

Esta cuestión ya expresamente resuelta en el artículo 588 ter c) último párrafo, que permite intervenir el dispositivo de terceros cuando estén siendo utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

¿Qué criterios deben manejarse a la hora de determinar la extensión de la medida? ¿cómo debe motivarse? ¿se puede autorizar sin distinción la intervención de las comunicaciones y de todos sus datos asociados?

Esta pregunta va íntimamente ligada a la 7) y a la 35).

Una de las novedades más relevantes de la reforma es que la extensión de la medida tiene que estar concretada y determinada por el/a juez/a de instrucción. Se ha acabado con la práctica anterior de entender que la intervención telefónica se extendía necesariamente a todos los datos electrónicos asociados a las comunicaciones intervenidas, y por tanto la autorización judicial lo abarcaba todo, en atención a la importancia de dispensar protección constitucional al cúmulo de información personal derivada de los instrumentos tecnológicos de nueva generación (STC 173/2011). Ahora es el/a juez/a quien deberá ponderar qué es lo que necesita y cómo acceder a ello, identificando con todo detalle el nivel de injerencia –la extensión- de la medida que autoriza. Así lo exige el artículo 588 bis c) 3-c al disponer que la resolución judicial que autorice la medida tiene que determinar expresamente la extensión de la misma, especificado su alcance. Alcance que está delimitado en cada medida en particular.

En el ámbito de intervenciones telefónicas y telemáticas, el art. 588 ter b) establece que la intervención podrá autorizar el acceso:

- al contenido de las comunicaciones
- y a los datos electrónicos de tráfico o asociados al proceso de comunicación. Que son aquellos que se generen como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

- A los datos que se produzcan con independencia del establecimiento o no de una concreta comunicación en los que participe el sujeto investigado, ya sea como emisor o como receptor,

Y en este sentido, el 588 ter d.2) establece que para determinar la extensión de la medida (588 bis 3-c)), la solicitud de autorización judicial podrá tener por objeto alguno de esos extremos:

- El registro y grabación del contenido de la comunicación, indicando el tipo y a forma de comunicaciones a las que afecta.
- El conocimiento de su origen o destino de la comunicación.
- La localización geográfica del origen o destino de la comunicación
- El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación.

En el ámbito del registro de dispositivos de almacenamiento masivo de información, el 588 sexies c) exige que el auto judicial mediante el que se acuerda el acceso a la información contenida en estos dispositivos fije los términos y el alcance del registro.

En el ámbito del registro remoto sobre equipos informáticos, el 588 septies 2-b) exige que el auto judicial fije el alcance de la medida, la forma en la que se procederá al acceso y la aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutara el control de la información.

En cuanto a los criterios que deben manejarse a la hora de determinar la extensión de la medida y cómo debe ser la motivación, como ya hemos dicho, en función de la información que pretenda obtenerse se determinará la extensión de la medida, -en relación con la investigación concreta y con los resultados esperados- que deberá sujetarse a los mismos criterios rectores que para la adopción de la medida en cuestión. Dichos criterios rectores están contenidos en el artículo 588 bis a) y son, especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Y como dice la Exposición de Motivos de la LO 13/2017, la proclamación normativa de los principios que el Tribunal Constitucional ha definido como determinantes de la validez del acto de injerencia. Toda medida deberá responder al principio de especialidad. Ello exige que la actuación de que se trate tenga por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose pues las medidas de investigación tecnológica de naturaleza prospectiva, de acuerdo con el concepto que informa la doctrina emanada del máximo intérprete de la Constitución, por todas la sentencia 253/2006, de 11 de septiembre. Las medidas de investigación tecnológica deben además satisfacer los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora. Estos principios están explicados en el precepto referido, 588 bis a).

¿Se pueden distinguir diferentes niveles de protección según se trate de datos de contenido, tráfico o de usuarios? ¿qué valores constitucionales se ven afectados en cada caso? ¿cuáles son las consecuencias de su respectiva protección constitucional? ¿Se transforma el régimen de garantías según haya finalizado o no el proceso comunicativo?

Así lo tiene establecido nuestra jurisprudencial constitucional destacando distintos niveles de afectación de valores constitucionales, sometidos a diferentes regímenes de garantías, que en ocasiones no resulta sencillo deslindar en compartimentos estancos, sino que a veces se solapan o sobreponen. De ahí, por ejemplo, que el TJUE en las SSTJUE de 8/4/214 y 21/12/2016 analicen el régimen de garantías de los datos conservados por los prestadores de servicios tanto desde la perspectiva del art. 7 (respeto a la vida privada y familiar, domicilio y comunicaciones) como del art. 8 (protección de datos de carácter personal).

Así, por ejemplo, como indica la STC 115/2013, de Pleno, de 9 de mayo, refiriéndose a la versatilidad tecnológica que han alcanzado los teléfonos móviles, con múltiples funciones indispensables hoy en día en la vida cotidiana, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.), son susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo al derecho al secreto de las comunicaciones (art. 18.3 CE), sino también a los derechos al honor, a la intimidad personal y a la propia imagen (art. 18.1 CE), al derecho a la intimidad, (art. 18.1 CE) e incluso al derecho a la protección de datos personales (art. 18.4 CE).
Precisamente nuestra CE marca diferencias en cuanto al régimen de garantías aplicable, exigiendo, en todo caso, en relación con el derecho al secreto de las comunicaciones (art. 18.3 CE), la salvaguarda judicial, esto es, la necesaria autorización judicial, frente a otras intromisiones en ámbitos -también privados- que no quedan sometidos necesariamente a la exigencia de previa autorización judicial.

Es decir, en nuestro sistema constitucional, la protección del derecho al secreto de las comunicaciones alcanza entidad propia que trasciende o supera la protección con la que ampara al derecho a la intimidad, ya que incluso las comunicaciones quedan protegidas con independencia de su contenido, esto es, con independencia de que lo comunicado tenga en realidad un carácter íntimo o de otro género, aclarando que el concepto de secreto tiene carácter formal (STC 114/1984, de 29 de noviembre, FJ 7; 34/1996, de 11 de marzo, FJ 4).

Además, el secreto de las comunicaciones protege no sólo el secreto de lo comunicado, sino que abarca también el proceso de comunicación (existencia misma de la comunicación y resto de circunstancias o datos externos de la misma: su momento, su duración, su origen o destino (STC 123/02, 281/2006, 230/07, etc; así

como las Sentencias del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, caso Malone c. Reino Unido, § 84 y, de 3 de abril de 2007, caso Copland c. Reino Unido, § 43, entre otras).

La obtención de dichos datos que quedan abarcados por el derecho al secreto de las comunicaciones protegido en el art. 18.3 CE, queda sometida, por expresa reserva constitucional, a un régimen de estricta autorización judicial (art. 18.3 CE), so pena de ilicitud (art. 11.1 LOPJ), de forma que la policía, ni siquiera en casos de urgencia, podrá proceder a su averiguación, sin previa autorización judicial.

Esta diferenciación, en cuanto a régimen de garantías aplicable, no aparece en los textos internacionales (art. 8 CEDH, o art. 7 y 8 de la Carta de Derechos Fundamentales de la Unión), de manera que la recepción de los esquemas que tanto la jurisprudencia del TEDH como la del TJUE vienen manejando, requieren un tratamiento cauteloso, dado que en la labor interpretativa que ejercen dichos Tribunales internacionales no se ven forzados a efectuar tal distinción, que, sin embargo, resulta inexcusable en nuestro ordenamiento nacional, a la hora de determinar si nos encontramos ante una intromisión en el derecho al secreto de las comunicaciones, o de otro tipo, para así comprobar y determinar el régimen de garantías aplicable, existiendo supuestos dudosos o fronterizos, respecto a los cuales la jurisprudencia se ha mostrado, en ocasiones, vacilante, en cuanto al régimen de garantías aplicable.

Resulta, por tanto, necesario deslindar los supuestos de afectación al derecho al secreto de las comunicaciones frente a otro tipo de injerencias que afecten exclusivamente al derecho a la intimidad u otros derechos fundamentales, respecto a los cuales, aunque también rige como regla general la necesidad de resolución judicial por tratarse de una medida limitativa de un derecho fundamental, no obstante, debido a la falta de exigencia expresa constitucional de autorización judicial, la policía judicial podrá acordar dichas intromisiones que constituyan una injerencia **LEVE** en la intimidad de las personas (STC 115/2013), sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 70/2002, de 3 de abril, FJ 10; 123/2002, de 20 de mayo, FJ 4; 56/2003, de 24 de marzo, FJ 2; 281/2006, de 9 de octubre, FJ 4; y 142/2012, de 2 de julio, FJ 2).

En este sentido, conviene traer a colación diversos pronunciamientos de nuestro TC, que nos ayudarán en esta tarea diferenciadora:

En la STC 70/2002, el TC abordó la distinción del derecho al secreto de las comunicaciones postales, por un lado, y del genérico derecho a la intimidad, por otro. El recurrente alegaba vulneración del secreto de las comunicaciones al habérsele intervenido una "carta" (en realidad eran unas hojas de papel manuscritas y dobladas, sin envoltorio o sobre), que la Guardia Civil halló en el interior de una agenda, y desdobló y leyó sin previa autorización judicial.

En el supuesto examinado, el TC tomó en cuenta dos circunstancias relevantes: la primera, que la supuesta "carta" no presentaba ninguna evidencia externa que hubiera permitido a la Guardia Civil "ex ante" tener constancia objetiva de que aquello había sido objeto de una comunicación postal secreta tutelada por el artículo 18.3 CE. En segundo lugar, consideró que la intervención del papel no había interferido en el proceso de comunicación mientras éste estaba teniendo lugar, sino que el proceso de comunicación ya se había consumado anteriormente.

Esas dos circunstancias (falta de constancia "ex ante" de que lo intervenido hubiera sido en su momento objeto de una comunicación secreta por carecer en el momento de la intervención de envoltorio o sobre, y la falta de interferencia en el proceso de comunicación en el mismo momento en el que se está produciendo) resultaron decisivas, en opinión del TC, para excluir que el papel intervenido pudiera quedar cubierto por el derecho al secreto de las comunicaciones, declarando en la STC 70/2002 que la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se llevará a cabo, en su caso, a través de las normas que tutelan la intimidad u otros derechos.

Esta última afirmación, sin embargo, dio lugar a interpretaciones equívocas en cuanto a su alcance, que fue precisado en la posterior STC 123/02, aclarando que el secreto de las comunicaciones abarca también los datos que hayan quedado registrados en el momento en el que se está produciendo el proceso de comunicación, aunque se tomen en consideración una vez finalizado el acto comunicativo, extendiendo el TC la protección específicamente prevista en el art. 18.3 CE –necesidad de autorización judicial- a los listados de llamadas efectuadas desde un teléfono fijo (en el mismo sentido la STC 230/07 respecto del listado de llamadas contenidas en la memoria de un teléfono móvil), pues no otra interpretación cabía decantar de la jurisprudencia emanada por el TEDH en los ya referidos casos Malone y Copland, entre otros.

Otro dato a tomar en consideración en la tarea delimitadora podemos extraerlo de la STC 173/11, de 7/11 (aunque posteriormente fue anulada por STEDH Trabajo Rueda c. España de 30/05/2017) en la que se exponía lo siguiente: *"(…) A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado".*

La dicción literal podría sugerir que los mensajes efectivamente enviados, o ya leídos, perderían la protección del específico derecho al secreto de las

comunicaciones, para pasar a formar parte del genérico derecho a la intimidad, con la importante repercusión en el régimen de garantías que conlleva.

Pero las SSTC 142/12, de 2/7, 241/12, de 17/12, y finalmente la STC 115/13, de Pleno, de 9 de mayo, parece que nuevamente vienen a aclarar la cuestión, al afirmar de forma concluyente, que *"el derecho al secreto de las comunicaciones (art. 18.3 CE) consagra tanto la interdicción de la interceptación como el conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado no sólo por la interceptación en sentido estricto —aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación— sino también por el conocimiento antijurídico de lo comunicado, como puede suceder, sin ánimo de exhaustividad, en los casos de apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil".*

La STC 142/12, de 2/7, y STC 115/13, de 9 de mayo, describen como criterio para descartar la vulneración del derecho al secreto de las comunicaciones, el que los datos –de un listado de contactos de una agenda de un teléfono móvil- *"no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación* ***pretéritos*** *o* ***futuros****"* (STC 142/2012, FJ 3).

La inclusión de los actos de comunicación "pretéritos", en los términos expuestos por las STC 123/02, 230/07, y otras, no parece plantear mayor objeción, pues así se desprende de la doctrina esencial emanada por el TEDH. Sin embargo, la referencia a actos de comunicación "futuros" parece una extensión novedosa de su ámbito objetivo, si se pone en relación con anteriores pronunciamientos del propio TC. Por ejemplo, la STC 137/2002, de 3 de junio, FJ 3, que indicaba que cualquier objeto –sobre, paquete, carta, cinta…– que pueda servir de instrumento o soporte de la comunicación postal no será objeto de protección del derecho reconocido en el art. 18.3 CE si en las circunstancias del caso no constituyen tal instrumento de la comunicación, o el proceso de comunicación no ha sido iniciado (STC 137/2002, de 3 de junio, FJ 3); así no constituyen objeto de este derecho cuando se portan por su propietario o terceros ajenos a los servicios postales, o viaja con ellos, o los mantienen a su disposición durante el viaje.

En la STC 70/2002 consideró, en ese caso concreto, que el papel intervenido no merecía la protección constitucional dispensada a la correspondencia, pero el fundamento de la exclusión no se basaba en el simple dato de que el proceso de comunicación ya se había consumado, sino en el hecho de haberse despojado del continente, sin rastro alguno del proceso comunicativo, por lo que la averiguación del contenido del escrito que en su día pudo haber sido objeto de correo postal no implicaba la averiguación de datos registrados en el momento en el que la comunicación tuvo lugar.

Se descarta con ello, a nuestro juicio, que la desprotección de las comunicaciones “pretéritas” pueda producirse por el simple hecho de que el mensaje haya sido abierto y leído por su destinatario, pues esta circunstancia, lo mismo que sucede cuando la llamada telefónica ha finalizado, no conlleva la desprotección de los datos que pretendan averiguarse, si estos se han originado o registrado en el momento en el que el proceso de comunicación está teniendo lugar –como ocurre con el listado de llamadas telefónicas (STC 123/02), o el registro de llamadas de un teléfono móvil (STC 230/07), o de forma análoga en la carpeta de correo electrónico, o una carta abierta que aún se halle en el interior de un sobre o envoltorio que incorpore los datos externos de la comunicación postal-, pues el secreto de las comunicaciones se proclama con independencia de que esos datos se averigüen una vez finalizado el proceso comunicativo.

Precisamente, la STC 230/07 razona que los listados de llamadas contenidos en la memoria del teléfono móvil quedan igualmente amparados por el secreto de las comunicaciones, toda vez que el acceso y registro de los datos que figuran en dichos listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones (SSTC 123/2002, de 20 de mayo, FJ 4, ó 56/2003, de 24 de marzo, FJ 2, y SSTEDH de 2 de agosto de 1984, caso Malone c. Reino Unido, § 84 y, entre las últimas, de 3 de abril de 2007, caso Copland c. Reino Unido, § 43), de la misma forma que la STC 123/02 había establecido años antes que la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requería resolución judicial, pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que quedaba comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE que requiere autorización judicial.

En efecto, los listados telefónicos *incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y a su duración, para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar, con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso a efectos, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión* (en este mismo sentido STC 281/06).

Consideramos, como conclusión lógica de la doctrina constitucional citada, que el hecho de que el mensaje haya sido leído, o la llamada telefónica haya finalizado, o en definitiva, que el proceso de comunicación haya concluido en sí mismo, no conlleva la desprotección de los datos que pretenden averiguarse si éstos se han originado o registrado en el preciso momento en que el proceso de comunicación está teniendo lugar –como ocurre con el listado de llamadas telefónicas, o la agenda de llamadas de un teléfono móvil-, pues el secreto de las comunicaciones se proclama con independencia de que esos datos se traten de averiguar una vez finalizado el proceso comunicativo.

En efecto, en la STC 123/02 ya expuso el TC que el listado de llamadas telefónicas se halla protegido por el derecho al secreto de las comunicaciones por incidir en la vertiente externa del acto comunicativo, sometida por ello en nuestro ordenamiento jurídico a reserva judicial (art. 18.3 CE), analizando en dicha STC 123/02 la adecuación constitucional de una simple providencia que acordaba la entrega a la Policía por parte de la compañía telefónica de los listados de llamadas telefónicas procedentes del teléfono de un inculpado, tras solicitud en este sentido formulada por la Policía. Desde esta perspectiva, aun considerando el TC que desde luego la resolución judicial debía haber adoptado la forma de Auto, excepcionalmente admitió que una providencia, integrada con la solicitud a la que se remite, podía cumplir las exigencias constitucionales en un caso como el analizado en el que se trataba de autorizar el acceso a los listados telefónicos por parte de la policía, destacando a estos efectos el dato de la menor intensidad lesiva en el objeto de protección del derecho al secreto de las comunicaciones que el acceso a los listados comporta, pero no por ello deben quedar menos protegidos, ni excluidos del régimen de autorización judicial previa obligatoria.

En el caso objeto del recurso de amparo en la STC 123/02, de la integración de la providencia con la solicitud de acceso a los listados de los teléfonos, resultaban los elementos que son exigibles desde la perspectiva constitucional: los hechos investigados, el delito que podían constituir, los datos de los teléfonos y los hechos de que los que se inferían las sospechas, concluyendo que más allá de la ausencia de ponderación que, en principio y formalmente, es predicable de las providencias, sin embargo, en el caso concreto –por remisión al oficio policial- existió la resolución judicial requerida por el art. 18.3 CE para legitimar la limitación del derecho fundamental al secreto de las comunicaciones.

A diferencia del Ministerio Fiscal, ¿puede solicitar una intervención telefónica el resto de acusaciones? ¿Cómo se gestionaría el secreto en ese caso?

Hay opiniones al respecto. En principio, el artículo 588 bis b) al que se remite el 588 ter d) establece que la solicitud de autorización judicial para acordar alguna de las medidas del Capítulo IV de la Lecrim, solamente puede pedirla el Ministerio Fiscal o la policía judicial. Por lo que en atención a la literalidad del precepto que excluye la posibilidad de petición de cualquier otro interviniente en la causa, se argumenta que no cabe que la intervención telefónica la solicite otra acusación, lo que es congruente con el secreto sumarial. Sin embargo, hay otra posición que se plantea la posibilidad de solicitud de la medida por otra acusación distinta al Ministerio Fiscal, al amparo de lo dispuesto en el artículo artículo 311 Lecrim que establece que el juez que instruya el sumario practicará las diligencias que le propusieran el Ministerio Fiscal o cualquiera de las partes personadas, si no las considera inútiles o perjudiciales, y que en este caso se podría gestionar el secreto de manera que no tuviera ya acceso a dicha pieza separada. O bien que el/a juez/a de instrucción la acuerde de oficio asumiendo la

“petición” de la acusación, si se entiende que no pueden solicitarla peor sí ponerlo en conocimiento del/a juez/a y que la acuerde de oficio tras oír al Ministerio Fiscal.

En relación con la notificación a terceros ¿qué debe entenderse por imposibilidad, esfuerzo desproporcionado, o perjuicio para futuras investigaciones?

El art. 588 ter i-3) dispone que *se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones.*

Este precepto ha suscitado mucha polémica. En principio, según el tenor literal de este precepto debería notificarse a cualquier persona que interviene en la comunicación interceptada, lo que se considera por lo/as asistentes al seminario como materialmente imposible. Se podría incorporar un criterio interpretativo con el fin de racionalizar este deber de notificar a terceros. Por ejemplo, en el Anteproyecto de Ley procesal penal de 2011, en su art. 286 concretaba las personas a quienes se debía notificar la resolución judicial que ordenó la intervención de las comunicaciones: a) al investigado, b) al titular o usuario del medio de comunicación o telecomunicación que haya sido afectado por la medida y c) a los participantes den las telecomunicaciones intervenidas pero cuando *su intimidad se haya visto seriamente afectada por la medida y siempre que hayan sido identificados.* También se introduce un criterio más racional en el Manuel “La reforma de la Lecrim en 2015” de Manuel Marchena y Nicolás González-Cuéllar, como que esta notificación al menos se haga con aquellas personas inicialmente investigadas y sospechosas que han padecido una interceptación en sus comunicaciones, pero que luego no han sido llamadas al proceso.

El precepto no concreta cuándo debe llevarse a cabo dicha notificación. Entendemos que cuando se ha alzado el secreto.

¿A quién alcanza el deber de colaboración de los prestadores de servicios previsto en el art. 588 ter e? ¿Cuál es el alcance y la extensión del deber de colaboración contemplado en el artículo 588 septies b)? ¿Podrían oponerse? ¿Cómo? ¿en qué casos?

La nueva regulación recoge el deber de colaboración con Jueces, Ministerio Fiscal y Policía Judicial -arts. 588 bis c) apartado 3.h), 588 ter e), 588 ter k), 588 quinquies b), 588 septies b), 588 octies- que se extiende a toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. Es decir, tal deber de colaboración se extiende a otras personas físicas o jurídicas distintas de las operadoras convencionales, dada la existencia de redes alternativas de comunicación que pueden actuar como canalizadores del tráfico.

Se trata, por tanto, de una obligación dirigida a cualquier persona física o jurídica, sea o no operadora de servicios, que por una u otra razón, disponga de datos o informaciones concretas incluidas en un sistema informático de almacenamiento.

Como indica MARCHENA GÓMEZ nace así la categoría legal de "sujetos obligados", no necesariamente vinculada a la prestación de un servicio de telecomunicaciones, que se asocia a la condición de sujeto en cuyo poder obre un sistema informático de almacenamiento, y que nace a partir del requerimiento de conservación formulado por el Fiscal o los agentes facultados.

La obligación de atender a ese requerimiento policial se subordina a la posibilidad de un cumplimiento que no exija del afectado una actuación que vaya más allá de lo exigible. Los derechos del acusado a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE,) justifican la excepción que se consagra a favor del propio investigado en el art. 588 septies b), e igualmente respecto de las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional. Consideramos que esta disposición contenida específicamente en los registros remotos sobre equipos informáticos es extensible al deber de colaboración del 588 ter e). El deber de colaboración exige deber de secreto y la negación a colaborar podría integrar un delito de desobediencia.

La asistencia o deber de colaboración puede ir dirigido al acceso al sistema, a facilitar el examen o visualización, o incluso a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos, que facilite la información que resulte necesaria para el buen fin de la diligencia.

En cuanto al alcance de ese deber de colaboración, solamente se menciona como límite a dicho deber, que el mismo suponga una carga desproporcionada para el afectado, como menciona el artículo 588 sexies c) en el ámbito del registro de dispositivos de almacenamiento masivo de información. No parece que tal deber pueda llegar al extremo de obligar a un fabricante u operadora a diseñar un software que sea preciso para quebrantar el acceso o la protección de datos encriptados, sino que debe tratarse de información preexistente, accesible y disponible.

Recomendamos un artículo muy interesante de Javier Hernández García en la revista Información y Debate nº 85, sobre Apple vs. FBI, cuando Apple se negó a prestar su colaboración de forma activa negándose a la creación de un software tendente a acceder a los contenidos encriptados del IPhone de un presunto terrorista.

Si los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, se niegan a facilitar a la policía judicial los datos de titularidad de un número de teléfono o de cualquier otro medio de comunicación o los datos identificativos de cualquier medio de comunicación, ¿Deben ordenarlos los Jueces cuándo la ley no lo exige?

El artículo 588 ter m) LECRim establece que cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

Sucede, con cierta frecuencia, que los prestadores de servicios rechazan facilitar, sin previa autorización judicial, alguno de los datos identificativos, por ejemplo, el IMEI, pues salvo supuestos en los que el terminal haya sido vendido por el mismo prestador de servicios, los datos identificativos del IMEI, según alegan los proveedores de servicios, deben buscarse de forma entrecruzada vinculado al IMSI, esto es, quedando registrado en el momento en que hay una comunicación.

De ser eso así, o de existir cualquier otra causa que el proveedor de servicios justifique adecuadamente, resultará preciso acudir al artículo 588 ter j), que permite la averiguación, previa autorización judicial, de los datos vinculados a procesos de comunicación.

La STS 523/2017 se refiere expresamente al art. 588 ter m) considerando que hay una distinción entre datos que no son propios de la comunicación, en la medida en que el acceso a dichos datos no incide sobre la comunicación misma sino posteriormente cuando ésta ha ya finalizado, de aquellos datos que están vinculados a procesos de comunicación y que solamente podrán ser cedidos para su incorporación al proceso con autorización judicial. La sentencia referida resulta interesante porque el recurrente alegó que no había autorización judicial para que las compañías telefónicas entregasen a los agentes policiales los datos relativos a la identidad de las personas que comunicaban telefónicamente con los usuarios de los teléfonos intervenidos. El Tribunal Supremo considera que la autorización de intervención telefónica incluye por sí misma la posibilidad de conocer los números de teléfono que contactan con los intervenidos. Y que de ellos no resulta directamente la identidad de los titulares de esas líneas, pero que estos datos no son datos propios de la comunicación y que con la reforma ahora ya son datos que pueden solicitar los agentes directamente a las compañías telefónicas.

¿Alcanza el deber de colaboración a las entidades públicas o privadas que se encuentran ubicadas en el extranjero?

Debemos partir de la eficacia territorial de las leyes nacionales, restringida, como regla general, al territorio donde el Estado ejerce su soberanía, por lo que una entidad pública o privada ubicada en el extranjero no se halla sometida a las leyes ni a la jurisdicción de los tribunales españoles, ni por tanto puede ser considerada como sujeto pasivo del deber de colaboración previsto en el art. 588 ter e LECRim, ni perseguida por delito de desobediencia en caso contrario.

Cuestión distinta es que los tribunales españoles puedan dirigirse a las autoridades judiciales de otro país para su obtención, a través de los mecanismos de cooperación judicial penal.

Hoy en día, la obtención de datos de las grandes compañías, ubicadas a menudo en Estados Unidos, se viene produciendo sobre una base voluntaria, no fiscalizable ni sancionable en caso de incumplimiento, salvo por los autoridades del país donde se encuentran.

Podemos traer a colación un caso interesante examinado en Bélgica, conocido como caso Yahoo, en el que el Tribunal Supremo belga resolvió en fecha 1 de diciembre de 1015 que esta compañía aunque estaba registrada en California (USA) quedaba obligada a facilitar a las autoridades belgas la información de usuarios requerida, sometida en otro caso a las sanciones previstas en el artículo 46 bis del Código Procesal Criminal belga, sin que ello constituyere un ejercicio extraterritorial de jurisdicción. Las razones que adujo el citado tribunal es que se trataba de un operador que suministraba un servicio activo en Bélgica, con presencia en territorio belga, poseía un dominio .be, y que voluntariamente se sujetaba por sí mismo a la ley belga, mostrando publicidad basada en la localización de los usuarios de sus servicios.

En este sentido, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, establece en su art. 2 que dicha Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos, contemplando en el art. 3 la posibilidad de aplicación a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a determinadas materias que han sido objeto de armonización por medio de Directiva 200/21/CE.

¿Cómo debe procederse en caso de "hallazgo casual"?

Debemos tomar como punto de partida que el hecho punible cuyo esclarecimiento se persigue mediante la adopción de este tipo de medidas injerentes

ha de ser definido con unos contornos suficientemente nítidos, excluyentes de toda idea de prospección genérica o indefinida.

Pero en el caso de que con motivo de la investigación inicial se descubra casualmente otro delito, se introducen diversas cautelas en la nueva regulación, exigiendo ahora, en cualquier caso, que la continuación de la medida injerente para la investigación del delito casualmente descubierto una nueva autorización del juez que resulte competente para la investigación del delito casualmente descubierto. Es decir, no basta la autorización inicial, sino que precisará una nueva autorización que ajuste el nivel de sacrificio del derecho fundamental a los presupuestos constitucionales que le confieren legitimidad, lo que deberá decidir el Juez competente.

En este sentido, el art. 579 bis.1 LECRim establece como regla general que el resultado de la detención y apertura de la correspondencia escrita y telegráfica o de otras medidas injerentes de las comunicaciones telefónicas y telemáticas podrá ser utilizado como medio de investigación o prueba en otro proceso penal. En el trámite parlamentario, no se acogió la redacción inicial que recogía una cautela restrictiva exigiendo para ello que "*se tratase de un delito respecto del cual podría haberse acordado la medida"*.

Esa nueva autorización, tal y como expresamente establece el art. 579 bis.3 LECRim, exige una nueva evaluación del *marco* en el que se produjo el hallazgo casual, comprobando también la *imposibilidad* de haber solicitado la medida que lo incluyera en su momento, a fin de evitar solicitudes fraudulentas. El Juez competente para resolver sobre la nueva autorización podrá ser el mismo que otorgó la autorización inicial, en el mismo u otro procedimiento, según concurra o no conexidad, u otro Juez diferente que resulta competente en virtud de las reglas de atribución de competencia.

Asimismo el Juez deberá informar al juez competente si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.

Si se trata de informaciones que afectan a investigaciones que deban desarrollarse en el extranjero podrá acudirse al intercambio espontáneo de información o a la denuncia con efectos procesales, previstos en los convenios y restos de instrumentos de cooperación judicial en materia penal, y en caso de urgencia, a través de Interpol.

Esta nueva previsión resulta acorde con reiterada jurisprudencia constitucional y de la Sala II del TS recaída en esta materia. La STC nº 41/1998, de 24 de febrero, afirmó que el que se estén investigando unos hechos delictivos no impide la persecución de cualesquiera otros distintos que sean descubiertos por casualidad al investigar aquellos, pues los funcionarios de policía tienen el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuviera

conocimiento, practicando incluso las diligencias de prevención, en cumplimiento de la obligación que le imponen los arts. 282 y 286 de la LECRim, y el art.11 g) de la Ley Orgánica de Cuerpos y Fuerzas de Seguridad del Estado de 13 de marzo de 1986. [STS 1577/2001, de 12 de septiembre]

En este sentido, la STS 1313/2009, de 16 de diciembre, estableció que los hallazgos casuales son válidos, pero la continuidad en la investigación de un hecho delictivo nuevo, casualmente detectado, requiere de una renovada autorización judicial.

La STS 102/2007, de 16 de febrero, en un asunto en el que se encontró casualmente droga y un arma (hallazgo casual) al ejecutar el mandamiento de entrada y registro dentro del proceso por delito fiscal y, tan pronto se advirtió su existencia, se suspendió la diligencia que se practicaba para dar cuenta al juez instructor que dictó en el mismo día un auto ampliatorio del objeto de la investigación, debidamente fundado, considera el TS que los indicios justificativos de la medida son aplastantes y las razones jurídicas que aconsejaban su adopción inobjetables. Añade que su regularidad formal estaría reforzada también, como apunta el Ministerio Fiscal, en caso de hallazgos casuales, por la flagrancia del delito (art. 553) o también acudiendo a la regla de la conexidad a que se refieren los arts. 17.5 y 300 L.E.Crim, teniendo en cuenta que no estaríamos ante un cambio o novación del objetivo inicial del acto de entrada y registro, sino ante una ampliación o adición al mismo, consecuencia de la prueba casualmente descubierta en una investigación judicial legítima.

La STS 412/2017 (ponente Sr. Palomo del Arco) establece:

Es cierto que no se pudo acreditar que el arma encontrada fuera la utilizada en el robo, pero ello no le privaría en cualquier caso, de integrar un hallazgo casual. La STS 717/2016, de 27 de septiembre recuerda con citas de las SSTS nº 1060/2013, de 23 de setiembre y 777/2012, de 17 de octubre, que: esta Sala Casacional ha declarado repetidamente que el hallazgo casual , es decir, el elemento probatorio novedoso que no está inicialmente abarcado por el principio de especialidad, puede ser utilizado en el propio o distinto procedimiento, bien por tratarse de un delito flagrante o bien por razones de conexidad procesal, siempre que, advertido el hallazgo, el juez resuelva expresamente continuar con la investigación para el esclarecimiento de ese nuevo delito, ante la existencia de razones basadas en los principios de proporcionalidad e idoneidad. El hallazgo no solamente se proyecta hacia el futuro, como en el caso de unas intervenciones telefónicas en donde resultan indicios de la comisión de otros delitos diferentes a los investigados, sino también puede producirse hacia el pasado, como cuando en el curso de un registro domiciliario, aparecen evidencias de otros ilícitos, o cuando, como aquí sucede, las intervenciones telefónicas pueden arrojar datos sustanciosos acerca de la participación de los comunicantes en hechos no inicialmente investigados por esa vía, con tal que, como hemos dicho, tal línea de investigación sea puesta de manifiesto ante el juez, y éste, valorando los intereses en juego, acceda a su incorporación al

proceso, conjugando un elemental principio de proporcionalidad. Se trata, en suma, de aquellos descubrimientos casuales que pueden aportar luz para el esclarecimiento de los hechos, de carácter novedoso (puesto que permanecían ocultos), y que han de ser investigados, con tal que la autoridad judicial pondere su importancia, salvaguarde el principio de especialidad, y justifique su necesidad y proporcionalidad.

En palabras de la STS 616/2012, de 10 de julio, por la denominada doctrina del hallazgo casual se legitiman aquellas evidencias probatorias que inesperadamente aparecen en el curso de una intervención telefónica, eventualmente en un registro domiciliario, de forma totalmente imprevista, aunque la doctrina de esta Sala Casacional, ha exigido que, para continuar con la investigación de esos elementos nuevos y sorpresivos, se han de ampliar las escuchas, con fundamento en el principio de especialidad, a través del dictado de una nueva resolución judicial que legitime tal aparición, y reconduzca la investigación, con los razonamientos que sean precisos, para continuar legalmente con la misma. Ya hemos visto que esto es lo que ha ocurrido en el caso de autos. En el propio sentido, la STS 768/2007, de 1 de octubre, declara que la doctrina de esta Sala ha entendido que el hecho de que el hallazgo de elementos probatorios de un determinado delito se produzca en el curso de la investigación autorizada para otro delito distinto no supone la nulidad de tal hallazgo como prueba de cargo. Y en la STS 885/2004, de 5 de julio, se decía que "las Sentencias de esta Sala, 1004/1999, de 18 de junio, y 1990/2002, de 29 de noviembre, sientan la doctrina de que si el hallazgo es casual, no por ello deja de tener valor lo encontrado, siempre que estemos en presencia de flagrancia delictiva...".

La STS 2110/2010, de 29 de abril, recoge:

Por tanto rige el principio de especialidad que justifica la intervención solo al delito investigado (STS. 3.10.96) pero los hallazgos delictivos ocasionales son "notitia criminis", sin perjuicio de que en el mismo o en otro procedimiento se amplíe o no la medida a seguir investigando el nuevo delito (SSTS. 31.10.96, 26.5.97, 19.1 y 23.11.98). En este sentido la STS. 792/2007 de 30.5, recuerda que como señaló la sentencia 276/96 de 2.4, en estos supuestos en que se investiga un delito concreto y se descubre otro distinto, no puede renunciarse a investigar la notitia criminis incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello pueda hacer precisa una nueva o específica autorización judicial o una investigación diferente de la del punto de arranque. Otra cosa significaría por ejemplo, la impunidad de un grave asesinato que se descubriera en un domicilio registrado o en una intervención telefónica acordada para descubrir estupefacientes para el tráfico o acreditar productos de receptación. Así dice la referida resolución: "Especialidad; principio que significa que "no cabe, obviamente, decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos" y que "no es correcto extender autorización prácticamente en blanco", exigiéndose concretar el fin del objeto de la intervención y que éste no sea rebasado. Lo que también ha sido matizado en el sentido de que no se vulnera la especialidad y ésta se da cuando no se produce una novación del tipo penal investigado, sino una adición o suma (SS.TS. 2 de julio de

1993 y 21 de enero de 1994); así como que no puede renunciarse a investigar la "notitia criminis" incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello hace precisa una nueva autorización judicial específica o una investigación diferente de la que aquélla sea mero punto de arranque (STS. 15 de julio de 1993)."

¿En qué se basa la doctrina del "silencio estratégico"? ¿Cabe entenderla superada a la vista de la actual regulación?

Reiterada problemática ha venido planteando la impugnación de la validez y legitimidad de las injerencias acordadas en distinto procedimiento, ante la necesidad de que el Tribunal cuente con todos los elementos de juicio que determinen la constitucionalidad de la injerencia.

Esta cuestión fue abordada por la jurisprudencia del TS, en concreto, el Acuerdo de Pleno no jurisdiccional de 26 de mayo de 2009, en los siguientes términos:

"En los procesos incoados a raíz de la deducción de testimonios de una causa principal, la simple alegación de que el acto jurisdiccional Imitativo del derecho al secreto de las comunicaciones es nulo, porque no hay constancia legítima de las resoluciones antecedentes, no debe implicar sin más la nulidad.

En tales casos, cuando la validez de un medio probatorio dependa de la legitimidad de la obtención de fuentes de prueba en otro procedimiento, si el interesado impugna en la instancia la legitimidad, de aquel medio de prueba, la parte que lo propuso deberá justificar de forma contradictoria la legitimidad cuestionada.

Pero, si, conocido el origen de un medio de prueba propuesto en un procedimiento, no se promueve dicho debate, no podrá suscitarse en ulteriores instancias la cuestión de la falta de constancia en ese procedimiento de las circunstancias concurrentes en otro relativas al modo de obtención de las fuentes de aquella prueba."

La primera de las sentencias dictadas en desarrollo de ese acuerdo (STS 777/2009, de 24 de junio) expone que la nulidad de los actos procesales sólo puede basarse en algunas de las causas estrictamente reguladas el art. 238 de la LOPJ, y de admitir esa tesis se estaría alentando la creación de la nulidad presunta, categoría carente de cobertura en nuestro sistema procesal.

En palabras de la STS 187/2009, 3 de marzo "...ni el derecho a la presunción de inocencia ni el principio procesal "in dubio pro reo" llegan hasta el punto de tener que presumir por mandato constitucional que, salvo que se acredite lo contrario, las actuaciones de las autoridades son ilegítimas e ilícitas".

Concluye la STS 777/2009 que: "la lectura íntegra del acuerdo de 26 de mayo de 2009 conlleva: a) que no existen nulidades presuntas; b) que la prueba de la legitimidad de los medios de prueba con los que pretenda avalarse la pretensión de

condena incumbe a la parte acusadora; c) pese a ello, la ley no ampara el silencio estratégico de la parte imputada, de suerte que si en la instancia no se promueve el debate sobre la legalidad de una determinada prueba, esa impugnación no podrá hacerse valer en ulteriores instancias."

Este enfoque también cuenta con detractores, pues podrían estarse mezclando cuestiones de legitimidad constitucional, lo que puede afectar a la presunción de inocencia, como regla de enjuiciamiento, con otras atinentes más bien a los exigibles postulados de igualdad de partes y contradicción, imponiendo a la postre cargas procesales a la parte imputada, en materia de derechos fundamentales, que pudieran resultar poco respetuosas con la presunción de inocencia, como regla de tratamiento, siendo cierto además que hasta ese momento la cuestión suscitada no había sido objeto de un tratamiento uniforme, no faltando precedentes en una y otra dirección.

La STS nº 468/2016, de 31 de mayo, resolvió que la falta de constancia de la resolución habilitante que debió haber sido dictada en el procedimiento de origen, podía perfectamente ser denunciada por la defensa en el turno de intervenciones a que se refiere el art. 786.2 de la LECRIM. Dicha sentencia contó con un voto particular (Sr. Llarena Conde) que considera extemporánea dicha alegación, en la medida en que impedía al Ministerio Fiscal una reacción subsanadora; y con un segundo voto particular (Sr. Andrés Ibáñez), en el que sostiene que exigir a una defensa que exponga sus cartas a tiempo de que la acusación pueda prevenirse frente al uso posible de ellas, no es una cuestión de lealtad, sino que equivale a imponerle una actitud procesalmente suicida, "un -dialéctica y procesalmente aberrante- deber de colaboración con aquella en propio perjuicio".

La regla actualmente vigente introducida en la nueva redacción del art. 579 bis LECrim vendría, a nuestro juicio, a superar tal doctrina, pues para que el resultado de la medida injerente pueda ser utilizado como medio de investigación o prueba en otro proceso penal, se exige la deducción de testimonio de los particulares **necesarios para acreditar la legitimidad de la injerencia**, incluyéndose, en todo caso, entre los antecedentes indispensables, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.

Es decir, la nueva regulación exige la acreditación de la legitimidad de la injerencia en el procedimiento de destino mediante todos los antecedentes que resulten necesarios para ello.

Por este motivo, ante la previsión de tal deber legal de aportación de los antecedentes necesarios para acreditar la legitimidad de la injerencia, la doctrina del silencio estratégico pierde, a nuestro juicio, o cuando menos queda restringido su campo de aplicación.

En el debate suscitado en el seminario, algunos participantes estimaron que la doctrina del silencio estratégico podría seguir conviviendo con la previsión contenida en el art. 579 Bis LECRIM, exigiendo en cualquier caso la carga de suscitar el debate en la instancia. No obstante se alcanzó cierto grado de consenso al identificar que esta carga procesal que impone el acuerdo tiene más que ver con el principio de contradicción e igualdad de partes, que con la presunción de inocencia, que en cualquier caso exige la comprobación de las garantías que han rodeado la práctica de las pruebas que se afirman de cargo. De concluir que alguna o algunas de ellas han resultado lesivas de otros derechos fundamentales o carentes de garantías (art. 11 LOPJ), deben quedar excluidas del cuadro probatorio valorable, por así exigirlo también el derecho fundamental a un proceso con todas las garantías (art. 24.2 CE), identificando también que una de estas garantías, por su nueva incorporación al texto legal, determina la necesidad de aportación del testimonio de los **particulares necesarios para acreditar la legitimidad de la injerencia.**

Tal comprobación lógicamente debe en las partes acusadoras, a quienes corresponde, tal y como establecía el Acuerdo de 26 de mayo de 2009, la prueba de la legitimidad de los medios de prueba con los que pretenda avalarse la pretensión de condena, aunque la parte imputada nada alegue.

El juicio sobre la legitimidad de la medida no se agota en la constatación de la existencia de una inicial resolución judicial habilitante y de los autos de prórroga, sino también deberán analizarse las solicitudes policiales o del Fiscal, para comprobar las exigencias de necesidad, excepcionalidad y proporcionalidad.

Junto a ello todos aquellos documentos que puedan justificar la legitimidad de origen de la medida restrictiva también deberán ser aportados.

Se introduce, por tanto, una nueva garantía a fin de despejar en el proceso ulterior cualquier sombra de duda sobre la legitimidad de la injerencia y de la validez de la prueba que pretende proyectarse en un proceso distinto.

¿Se puede adoptar cualquier medida de investigación tecnológica, previa solicitud policial que se remite a fuentes confidenciales para motivar la base indiciaria?

La mera mención de fuentes confidenciales no es suficiente para justificar tal invasión en los derechos fundamentales y así se ha pronunciado la Sala II en numerosas ocasiones, como exponente la Sentencia 1497/2005, 13 de diciembre, en la que recuerda que las noticias o informaciones confidenciales, aunque se consideren fidedignas, no pueden ser fundamento, por sí solas, de una medida cautelar o investigadora que implique el sacrifico de los derechos fundamentales (cfr. STC 8/2000, 17 de enero). Igualmente, no será suficiente por regla general,

con la mención policial que se limita a justificar la petición en alusión a «fuentes o noticias confidenciales».

Si la confidencialidad está en el origen de la noticia policial de la perpetración delictiva, para justificar la medida, habrá de ir acompañada de una previa investigación encaminada a contrastar la verosimilitud de la imputación. Es decir, la confidencia puede servir de motor para la práctica de otras diligencias, que aporten auténticos indicios o sospechas, suficientes para justificar la medida de interferencia (así, véanse las SSTS de 15 de julio de 2013 y de 17 de diciembre de 2010 y las que en ellas se citan).

La STS 195/2014 respecto al valor del confidente, considera que para justificar actos invasivos en el espacio de libertad que reconoce nuestro texto constitucional, no vale el confidente por sí solo, es decir, no basta una desnuda remisión a las fuentes confidenciales. Las noticias o informaciones confidenciales no pueden ser fundamento por sí solas de una medida cautelar o investigadora que implique el sacrificio de los derechos fundamentales, sino que es necesario que vaya acompañada la confidencialidad de una previa investigación encaminada a contrastar la verosimilitud de la imputación (STC 8/2000).

Confidencia, investigación añadida y constatación que habrán de estar reseñadas en el oficio policial y que habrán de venir referidas tanto al indicio del delito como de su atribución a la persona a la que va a afectar la medida. En este mismo sentido se han expresado, entre otras muchas, las SSTS 1047/2007, 17 de diciembre y 25/2008, 29 de enero; 141/2013, 15 de febrero y 121/2010, 12 de febrero.

La constatación de la solidez de esos indicios es parte esencial del proceso discursivo y valorativo que debe realizar el Juez de Instrucción antes de conceder la autorización. El Instructor ha de sopesar el nivel de probabilidad que se deriva de los indicios. Sólo cuando éste adquiera ciertas cotas que sobrepasen la mera posibilidad, estará justificada la injerencia. No basta una intuición policial; ni una sospecha más o menos vaga; ni deducciones basadas únicamente en confidencias. Es necesario algo más, como también ha repetido el Tribunal Constitucional (STC 49/1999). Consideraciones similares pueden encontrarse en las SSTC 299/2000, de 11 de diciembre, ó 136/2000, de 29 de mayo, 8/2000, de 17 de enero.

En el caso de la STC 166/1999 la existencia de noticias confidenciales fue ponderada por el TC, junto a otros extremos, para entender que la autorización judicial de la medida --en aquel supuesto una intervención telefónica-- se había adoptado sobre la base de sospechas objetivas, que se sustentaban en un cúmulo de circunstancias de las que quedó constancia expresa en la resolución judicial integrada con la solicitud policial.

En el mismo sentido, la doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos ha admitido excepcionalmente la legalidad de la utilización de estas fuentes confidenciales de información, siempre que se utilicen como medios de investigación y no tengan acceso al proceso como prueba de cargo (Sentencia Kostovski, de 20 de Noviembre de 1989, Sentencia Windisch, de 27 de Septiembre de 1990):

"The Convention does not preclude reliance, at the investigation stage of criminal proceedings, on sources such as anonymous informants. However, the subsequent use of anonymous statements as sufficient evidence to found a conviction, as in the present case, is a different matter. It involved limitations on the rights of the defence which were irreconcilable with the guarantees contained in Article 6."

¿Cómo debe interpretarse el art. 588 ter i en lo relativo a la entrega de grabaciones a las partes?

El artículo *588 ter i)* dispone que *alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción se hará constar de modo expreso.*

Según dicho precepto, lo que se entrega a las partes es copia de las grabaciones excluyendo contenidos íntimos no relevantes. Se habla de copia de las grabaciones porque el SITEL es el original y solamente permite hacer copia (carece por sí de soporte original) ya que las conversaciones se registran en un ordenador central del que se extraen copias. Respecto del funcionamiento del sistema SiTEL resulta interesante la STS 554/2012 que explica que "*cualquier experto en tal sistema de interceptación de las comunicaciones suele explicar la regularidad del sistema en los términos siguientes u otros parecidos: el sistema SITEL (sistema de interceptación legal de las telecomunicaciones) diseñado para sustituir las carencias del anterior sistema de interceptación, se construye sobre la base de enlaces punto a punto con las Operadoras de telefonía, que transmiten la información correspondiente a la interceptación que dichas Operadoras realizan en su sistema, para almacenarse en el sistema central del Cuerpo Nacional de Policía. Los enlaces punto a punto establecidos, permiten únicamente la entrada de información procedente de la Operadora, la cual, automáticamente, es almacenada por el sistema central en el formato recibido, con características de solo lectura, sin intervención de los agentes facultados, y queda guardada con carácter permanente en el sistema central de almacenamiento a disposición de la Autoridad judicial. Para garantizar el contenido de la información dichos ficheros son firmados digitalmente, utilizando el formato de firma electrónico denominado PKCS#7 Detached, utilizando un certificado Camerfirma*

(como entidad certificadora autorizada) emitido por el Cuerpo Nacional de Policía y que se asocia a la máquina SITEL para que pueda firmar de forma desasistida los ficheros relativos al contenido e información asociada de la interceptación. Una vez que en el sistema central se realiza el proceso de firma, se genera un nuevo fichero que contendrá la firma electrónica, y que verificará tanto el contenido de la comunicación, como los datos asociados a la misma. Así, el sistema de firma electrónica nunca altera el contenido del archivo original que se está firmando. Los usuarios del sistema, los grupos operativos encargados de la investigación, no acceden en ningún momento al sistema central de almacenamiento, recogiendo únicamente un volcado de esa información con la correspondiente firma electrónica digital asociada, transfiriéndola a un CD o DVD para su entrega a la Autoridad judicial, garantizando de esta manera la autenticidad e integridad de la información almacenada en el sistema central". En base a todo ello ningún reparo cabe hacer al empleo de tal tecnología informática, por lo que cuando el juez ordena una intervención telefónica no impone la utilización de ningún sistema, sino que autoriza los más avanzados o los que en un momento dado utilice la policía judicial, siempre que ofrezcan plenas garantías, como es el sistema SITEL.

Se plantean varios problemas en la práctica: El primero de ellos el relativo a determinar quién debe filtrar el contenido de las partes de las grabaciones que se entregarán a las partes y el que se va a excluir por afectar a datos que no sean relevantes para el caso y puedan afectar a la vida íntima de las personas. Tiene que ser necesariamente el/a juez/a instructor, que es el garante de los derechos que se pueden ver afectados. Este extremo ha resultado ser muy controvertido en el seminario porque es una obligación que se considera materialmente imposible, ya que el/a juez/a no puede realizar en la práctica este filtro, ya que implica comprobar en todas las conversaciones si hay información sobre la vida íntima no relevante y para hacer la criba debe oír las copias.

¿Cabe reconocer expectativa razonable de privacidad en grupos de chat con numerosos componentes? ¿Cómo podemos delimitar lo público y lo privado?

La idea de la expectativa razonable de privacidad acuñada en la jurisprudencia de EEUU (Katz v. United States, Smith v. Maryland), ha sido también recogida por la jurisprudencia del TEDH y por nuestro TC a la hora de definir el alcance de la protección del derecho a la intimidad reconocido en el art. 18.1 CE.

En concreto, a fin de determinar si las nociones de "vida privada" y "correspondencia" son aplicables, el TEDH ha examinado en varias ocasiones si las personas tenían una expectativa razonable de que se respetaría y protegería su privacidad (Köpke v. Germany (dec.), N. ° 420/07, 5 de octubre de 2010).

Las SSTC nº 12/2012, de 30 de enero, y nº 170/2013, de 7 de octubre, se expresan en los siguientes términos:

"Un criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno. Así por ejemplo cuando se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores. Por el contrario, no pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean, claramente pueden ser objeto de registro o de información pública (SSTEDH de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido, § 57, y de 28 de enero de 2003, Peck c. Reino Unido, § 58)."

Las nuevas tecnologías ponen a disposición de los usuarios nuevas formas de comunicación, privadas, semiprivadas o públicas, inimaginables hace años, que pueden llegar a plantear dificultades para delimitar el ámbito de protección a la intimidad o al secreto de las comunicaciones. Por citar un ejemplo, las sesiones de chat en un foro abierto, en el que cualquier puede unirse simulando ser quien no es en realidad, contactando, por ejemplo, con un agente encubierto que simula un perfil correspondiente a un menor de edad, a quien efectúa proposiciones de carácter sexual. En ese caso, no existiría expectativa razonable de privacidad en relación con lo que el agente encubierto escucha o lee por sí mismo, pues el propio autor le trasmite sus manifestaciones en la sala de chat.

En el asunto United States v. Meregildo la Corte Suprema de EEUU consideró que tampoco puede considerarse que exista razonable expectativa de privacidad respecto a las publicaciones que una persona exponga, por ejemplo, en un perfil de facebook que sea visible únicamente para los amigos, aunque no sea completamente público, pues, aunque el acusado piense o confíe que su perfil no se va a compartir con la policía, no puede albergar la seguridad de forma justificable de que sus "amigos" vayan a mantener tal información privado.

Cuestión diferente sucede cuando se pretende averiguar las conversaciones que se produzcan dentro de un grupo de personas, incluso numeroso (p.e. grupos de whatssaps, etc.), en el que exista un control de acceso o facultad de excluir, es decir, no enteramente disponible al público. La intervención de las comunicaciones en este caso exigiría inexcusablemente autorización judicial, sin perjuicio de que cualquiera de sus componentes pudiera revelar espontáneamente los mensajes (sin concierto con la Policía para la obtención de conversaciones futuras, como veremos en la cuestión xxx).

En este mismo sentido, la Circular nº 1/2013 de la FGE considera que para que exista la protección del derecho al secreto de las comunicaciones o del derecho a la intimidad debe haber una expectativa razonable de privacidad y para ello es necesario que el medio sea adecuado y apto para permitir una comunicación secreta entre varias personas, lo que lleva a excluir los medios de comunicación de masas, salvo que permitan una conversación entre dos o más personas, pero "cerrada" o con disponibilidad para aceptar nuevos interlocutores (por ejemplo, video conferencias).

¿En qué supuestos es aplicable el plazo de 5 años para la conservación y destrucción de copias? ¿Qué finalidad cumple este plazo? ¿En qué supuestos cabría acordar excepcionalmente la conservación de las copias más allá de este plazo? ¿Qué garantías adicionales deberían establecerse?

La dicción del art. 588 bis k) LECrim, plantea diversas dudas:

Artículo 588 bis k. Destrucción de registros.

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

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

3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.

El precepto impone la destrucción de los registros originales que obran en poder de las Fuerzas y Cuerpos de Seguridad del Estado, y lo único que puede ser objeto de custodia son las copias custodiadas por el LAJ, esto es, dos soportes digitales distintos, uno contendiendo las grabaciones íntegras, y otro la transcripción de aquellos fragmentos que los agentes facultados consideren de interés, debiendo quedar bajo custodia temporal por el LAJ el primero de ellos.

Trascurridos cinco años desde que la pena se haya ejecutado debe procederse, como regla general, a su definitiva destrucción. Se plantea la duda si el plazo de cinco años ha de ser también observado a partir de la prescripción del delito o la pena, o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme.

En este aspecto los participantes del seminario se han mostrado divididos.

Si comparamos la dicción legal con la redacción inicial del Anteproyecto, resultaría que el plazo de cinco años únicamente es aplicable a los supuestos de ejecución de la pena, ya que en el anteproyecto se señalaba que Ia destrucción de las copias se acordaría cuando transcurrieran cinco años desde que la pena se haya ejecutado o el delito o la pena hayan prescrito".

Pero finalmente el art. 588 bis k) contiene dos proposiciones distintas, que permiten entender que están sometidas a distinto régimen temporal. Por un lado, en caso de ejecución de la pena, deberán trascurrir cinco años, y por otro, en caso de prescripción del delito o la pena, una vez declarada, se autoriza sin más la destrucción de las copias.

En la tramitación parlamentaria se añadieron otros dos supuestos de destrucción obligada, cuando se haya decretado el sobreseimiento libre, y cuando haya recaído sentencia absolutoria firme.

Esta interpretación nos parece más respetuosa con el derecho a la presunción de inocencia, como regla de tratamiento, sin tener que esperar en estos casos al trascurso de 5 años desde que se hayan adoptado dichas decisiones exoneratorias.

Como excepción, el tribunal podrá acordar su conservación, lo que deberá justificarse atendiendo a otros intereses constitucionalmente legítimos, dado que la mera conservación también constituye una limitación del derecho fundamental protegido, lo que aún resultaría más difícil de admitir en supuestos de sentencia absolutoria. La STEDH, caso Marper V. RU, de 4/12/2008, al analizar la conservación de datos de ADN y huellas dactilares de sospechosos absueltos o cuyas causas hayan sido sobreseidas, establece que la memorización de datos relativos a la vida privada de una persona constituye una injerencia en el sentido del artículo 8 del CEDH (Leander v. Suecia, 26 de marzo de 1987), independientemente de que los datos memorizados sean utilizados posteriormente o no (Amann v. Suiza). Afirma también que es particularmente preocupante el riesgo de estigmatización derivado del hecho de que personas no reconocidas culpables de ninguna infracción, que gozan, por lo tanto, del derecho a beneficiarse de la presunción de inocencia, sean tratados de la misma manera que las personas condenadas.

Quizá en supuestos de sobreseimiento libre que no conlleven efecto de cosa juzgada (por ejemplo, declaración de fallecimiento, o sentencia absolutoria únicamente respecto de alguno de los investigados), podría entenderse justificada la excepcional negativa del tribunal a su destrucción, que en buena lógica debería someterse a plazo en función de las razones que motiven su conservación.

¿Por qué debe llevarse a cabo el borrado y eliminado de estos datos?¿Quién debe ordenarlo?

El art. 588 bis k LECRIM, en su apartado 7, establece que una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida.

El acceso a tales datos se ha producido sobre la base de una autorización judicial emitida solamente con la finalidad de proceder a la investigación de unos hechos concretos, de ahí que todo el material obtenido queda íntegramente a la exclusiva disposición de la autoridad judicial. Es por ello que la jurisprudencia (STS 207/2012, de 12 de marzo, entre otras) ya venía exigiendo que los Tribunales, en las causas en las que se haya procedido a la realización de intervenciones telefónicas, deberán acordar de oficio en sus sentencias la destrucción de las grabaciones originales y de todas las copias que existan, conservando solamente de forma segura las entregadas a la autoridad judicial, y verificando en ejecución de sentencia, una vez firme, que tal destrucción se ha producido.

Se requiere, por tanto, que el órgano judicial de instancia, en línea con las resoluciones que ya venía dictando nuestro Tribunal Supremo, incluya entre los pronunciamientos de la sentencia que dicte, sea absolutoria o condenatoria, la **orden de borrado** de los archivos que obren en poder de las Fuerzas y Cuerpos de Seguridad.

Una vez han servido de elemento de prueba, su conservación policial debe cesar, correspondiendo a la Policía Judicial la ejecución material de la destrucción de archivos, pudiendo el Tribunal adoptar las cautelas que estime oportunas al respecto para asegurarse su cumplimiento. Únicamente serán conservadas las copias bajo custodia del Secretario Judicial.

Precisamente la exigencia de previsión legal específica relativa a la destrucción de los datos obtenidos constituye una de las garantías a las que se refiere expresamente el TEDH (Marper V. U.K. de 4/11/2008) en esta materia:

"It reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see, mutatis mutandis, Kruslin v. France, 24 April 1990, §§ 33 and 35, Series A no. 176-A; Rotaru, cited above, §§ 57-59; Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI; Association for European Integration and

Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, §§ 75-77, 28 June 2007; and Liberty and Others v. the United Kingdom, no. 58243/00, §§ 62-63, 1 July 2008).”

Como indica el Tribunal Supremo en su sentencia 565/2011, el borrado o eliminación lo ha de acordar el juez y han de velar por su cumplimiento los fiscales según su propia Circular, debiendo acordar también la destrucción de las copias que obren en poder de las Fuerzas y Cuerpos de Seguridad del Estado para eliminar cualquier tentación de su uso gubernativo. Podrán adoptarse las cautelas que se estimen oportunas para garantizar dicha operación.

Ante el silencio de la ley al respecto, ¿Cuál sería el régimen de impugnación por las defensas de las transcripciones de las conversaciones telefónicas grabadas o del volcado de los datos contenidos en un ordenador, USB, móvil…?

No existe un régimen legal expreso de impugnación, ya que el artículo 588 ter i) solamente indica que cuando se alce el secreto se entregará a las partes copia de las grabaciones y una vez examinadas podrán solicitar la inclusión en las copias de aquellas comunicaciones que entiendan relevantes y hayan sido excluidas. Por lo que literalmente este traslado a las partes se efectúa a los solos efectos de solicitar la inclusión en las copias de comunicaciones excluidas pro el/a juez/a. Sin embargo, nada obsta a que se pueda extender el ámbito material de este precepto y por tanto aprovechar este trámite para que las partes puedan realizar las impugnaciones que consideren convenientes, y por tanto, no habría inconveniente en entender que cuando se les entregue a las partes las copias y se les confiera un plazo para realizar alegaciones sobre la inclusión que pretendan de alguna conversación, puedan también interesar la exclusión de algún pasaje así como realizar alegaciones sobre la autenticidad o integridad de las grabaciones. De hecho, el Anteproyecto de Ley de Enjuiciamiento Criminal del 2011 en su artículo 287 preveía una comparecencia con las partes, una vez alzado, el secreto, para examinar las grabaciones y determinar los extremos relevantes excluyendo los que carecieran de interés, así como realizar las alegaciones oportunas sobre dichas grabaciones. Esta comparecencia podría sustituirse por una tramitación escrita, pero sería positiva en cuanto prevé un momento determinado para realizar las impugnaciones, sin perjuicio de lo que ya hemos dicho en la cuestión 14 a propósito del silencio estratégico, tratado en la STS 358/2016.

En cuanto a las causas de impugnación, no se regula nada al respecto con la reforma. De nuevo nos remitimos al Anteproyecto de Ley de Enjuiciamiento Criminal del 2011 sí exigía expresamente en su artículo 288 que las impugnaciones del contenido de las comunicaciones tendrían que basarse en la existencia de indicios objetivos de manipulación y solamente si los motivos de sospecha resultaban suficientes, el Tribunal acordaría la realización de una comprobación pericial sobre el funcionamiento del sistema utilizado y su posible manipulación. En cualquier caso sigue y consideramos que debe seguirse criterio jurisprudencial plasmado por ejemplo

en la sentencia del Tribunal Supremo 35872016, que establece que no basta una impugnación genérica sino debidamente razonada al no ajustarse a las exigencias de la buena fe procesal un cuestionamiento puramente estratégico y no concretado.

En cuanto a mecanismos para garantizar la autenticidad e integridad de las grabaciones, el artículo 588 ter f) exige un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, para asegurar la autenticidad e integridad de la in formación volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas. En concordancia con lo que decía la STS 358/2016 cuando refería sobre el sistema SITEL que *las acreditaciones individualizadas a los miembros de las unidades de investigación para acceder al sistema… únicamente permiten visualizar el contenido pero nunca modificarlo, son pues usuarios pasivos de la información. Y cumpliendo lo ordenado por la autoridad judicial proceden a volcar a un soporte, CD/DVD, el contenido de la intervención correspondiente, volcado que implica nueva certificación digital de cada soporte empleado con las siguientes precisiones: a) Ese volcado se realiza desde los centros remotos y utilizando los terminales del SITEL b) Se verifica de fecha a fecha, es decir, que comienza con el primer día de la intervención e incorpora la totalidad de las conversaciones y datos asociados producidos hasta la fecha que se indique al sistema, que será la señalada por el juzgado para que se le dé cuenta (semanal o quincenalmente) o la necesaria para solicitar la prórroga de la intervención. c) La realización de sucesivos volcados de la intervención a los soportes CD/DVD se lleva a cabo sin solución de continuidad, enlazando los periodos temporales hasta que finaliza la intervención, de forma que los CD/DVD aportados de esta manera al Juzgado contienen íntegramente la intervención correspondiente por lo que son los soportes que han de emplear para la solicitud de la prueba, en el caso de que sea necesario, para el acto del juicio oral. Desde un equipo remoto no es posible modificar ni borrar absolutamente nada del servidor central del SITEL. El soporte DVD en el que se vuelca la intervención telefónica se trata de un soporte de solo lectura, porque así lo han acordado llevar a cabo, es decir, se trata de un soporte en el que no se puede grabar sobre el mismo. d) Las transcripciones de parte de las conversaciones no implican más que una herramienta de facilitación del trabajo al Juez. El contenido de las conversaciones y datos asociados queda íntegramente grabado en el Servidor Central del SITEL, y no es posible su borrado sin autorización judicial específica, sin que sea posible su alteración porque queda registrado en el sistema cualquier intento de manipulación y ello de forma indeleble. La aportación de los soportes CD/DVD en los que se ha volcado la información, se efectúa por los responsables de las unidades de investigación y amparadas por la intervención que realiza el funcionario policial que actúa como secretario de las mismas. e) En cualquier momento del proceso es posible la verificación de la integridad de los contenidos volcados a los soportes CD/DVD entregados en el juzgado, mediante su contraste con los que quedan registrados en el Servidor Central del SITEL a disposición de la autoridad judicial. Este contraste puede realizarse por el juzgado en los terminales correspondientes para acreditar su identidad con la "matriz" del servidor central. La parte podría pedir esa verificación.*

Resulta interesante por otra parte recordar, como así hicimos en el seminario, una cuestión tan relevante como los requisitos exigidos para utilizar como prueba los resultados de una intervención telefónica. La STS 912/2016 detalla el protocolo de incorporación del resultado de la intervención al proceso como prueba de cargo susceptible por tanto de ser valorada. Y puede ser, a) la transcripción mecanográfica de las cintas, ya sea integral o sobre aspectos relevantes para la investigación, cotejada dicha transcripción bajo la fe del Letrado de la Administración de Justicia. Conviene aclarar que las transcripciones no son necesarias sino que es una forma de transferirlas a soporte papel para facilitar su consulta y constatación (STS 270/2017), aun que si se utilizan las mismas su autenticidad solamente valdrá si están debidamente cotejadas en la forma indicada. b) Audición de las cintas previa petición de las partes que no obstante pueden renunciar a dicha audición con la fórmula de darlas por reproducidas, siempre que dicha prueba se haya conformado con las debidas garantías y se haya podido someter a contradicción y que dicho proceder no conlleve una merma del derecho de defensa (TEDH caso Barberà, Messegué y Jabardó c. España). La reproducción en juicio es sustituible por el artículo 726 Lecrim (STS 20/2017). La STS 676/2012 refiere que la audición de las cintas no es requisito imprescindible para su validez como prueba y que el contenido de las conversaciones puede ser incorporado al proceso bien a través de las declaraciones testificales de los funcionarios policiales que las escucharon o a través de su trascripción mecanográfica como documental. Lo esencial en cualquier caso es la necesidad de preservar los principios de inmediación, contradicción y publicidad.

¿Encuentra amparo constitucional la regulación contenida en los artículos 588 ter d), 588 quinties b) y 588 sexies c), que permite a la Policía Judicial establecer medidas de vigilancia en casos de urgencia?

Tenemos la siguiente regulación:

Para las intervenciones telefónicas y telemáticas. Art. 588 ter d) 3.

- Delitos relacionados con la actuación de bandas armadas o elementos terroristas.
- Caso de urgencia
- Existencia de razones fundadas que hagan imprescindible la medida
- la podrá acordar el Ministro del Interior o en su defecto el Secretario de Estado de Seguridad
- Comunicación inmediata al/a juez/a de la adopción de la medida, y en todo caso, dentro de las 24 horas, haciendo constar las razones que la justificaron, la actuación realizada, la forma en la que se ha efectuado y su resultado.
- El/a juez/a tiene 72 horas para revocarla o confirmarla de forma motivada.

Para la utilización de dispositivos técnicos de captación de la imagen, seguimiento y localización. Art. 588 quinquies b) 4.

- No hay acotación de delitos.
- Caso de urgencia.
- Razones fundadas que hagan imprescindible la medida, explicando que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización, se frustrará la investigación.
- Podrá proceder a su colocación la policía judicial.
- Comunicación al/a juez/a, no ya inmediata, sino a la mayor brevedad posible, pero en todo caso en el plazo máximo de 24 horas.
- El/a juez/a podrá ratificar la medida o acordar su inmediato cese en el plazo máximo de 24 horas.
- Se menciona expresamente que la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso si el juez acuerda su cese inmediato.

Para el registro de dispositivos de almacenamiento masivo de información. Art. 588 sexies c) 4.

- No hay acotación de delitos.
- Urgencia.
- Existencia de un interés constitucional legítimo que haga imprescindible la medida (para determinar en qué consiste nos remitimos a la cuestión 23).
- Podrá llevarlo a cabo la Policía judicial que podrá por tanto examinar de forma directa los datos contenidos en el dispositivo incautado.
- Comunicación inmediata al/a juez/a, y en todo caso, dentro de las 24 horas, por escrito motivado haciendo constar las razones que la justificaron, la actuación realizada, la forma en la que se ha efectuado y su resultado
- El/a juez/a tiene 72 horas desde que fue ordenada la medida para revocar o confirmar la actuación policial, de forma motivada.

Esta posibilidad contemplada a propósito de las tres medidas de investigación referidas y que permiten la existencia de espacios policiales no sometidos en un primer momento al control judicial, ya que la intervención judicial se produce después de la injerencia en el derecho fundamental, no está exenta de problemas al caber la posibilidad de lapsos temporales de vigencia de la medida en cuestión ajenos al control judicial, por ejemplo cuando se adopta la medida y no se comunica al/a juez/a por cesarla antes de las 24 horas utilizándose para obtener información.

El fundamento constitucional en cada caso es diferente. En el caso de delitos relacionados con la actuación de bandas armadas o elementos terroristas, el fundamento se encuentra en el art. 55.2 CE, que establece la posibilidad de suspensión, en los términos que determine una Ley Orgánica, de los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. Por el contrario, la investigación urgente en materias que afecten a la

intimidad de las personas viene basada en la doctrina constitucional que delimita el art. 18.1 CE, a la que ya hemos hecho referencia en la cuestión nº 7.

Resulta muy interesante y así se expuso en el seminario, la STEDH caso Roman Zakharov c Rusia de 4 de diciembre de 2015, que establece el estándar mínimo que deben cumplir las legislaciones internas al regular las medidas secretas de vigilancia para evitar abusos de poder. Se debe establecer legalmente: la naturaleza de los delitos que pueden dar lugar a una orden de interceptación, las categorías de personas que pueden tener sus teléfonos conectados, un límite en la duración de la escucha telefónica, el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos, las precauciones que deben adoptarse al comunicar los datos a otras partes, y las circunstancias en que las grabaciones pueden y deben ser borradas o destruidas. Se especifica que en el examen y a supervisión de las medidas secretas de vigilancia pueden entrar en juego en tres etapas: a) cuando la vigilancia se ordena por primera vez, b) mientras se está llevando a cabo, o c) después de su terminación. En lo que respecta a las dos primeras etapas, la propia naturaleza y lógica de la vigilancia secreta impone que se efectúe sin el conocimiento del individuo. Por lo que ya que la persona afectada no podrá solicitar un recurso efectivo o participar en un procedimiento de revisión, es esencial que los procedimientos establecidos proporcionen garantías adecuadas para salvaguardar sus derechos, especialmente a través del necesario control judicial de la medida que ofrece las mejores garantías de independencia e imparcialidad. En cuanto a la tercera fase, tras la finalización de la vigilancia, la cuestión de la notificación posterior de las medidas de vigilancia está indisolublemente ligada a la eficacia de los recursos ante los Tribunales y por tanto a la existencia de salvaguardas efectivas contra el abuso de los poderes de control. En principio, la persona afectada no puede recurrir a los Tribunales, a menos que sea informada de las medidas adoptadas sin su conocimiento y por lo tanto pueda impugnar su legalidad de forma retroactiva. De ahí las exigencias de la necesaria notificación a terceros afectados por la medida recogida en la reforma analizada.

Si la medida adoptada por la Policía Judicial es posteriormente revocada por el Juez/a, ¿Qué sucede con la información obtenida? ¿Debe comunicarse a la persona afectada?

Entendemos que en los tres supuestos mencionados en la cuestión anterior, si el/a juez(/a acuerda su cese inmediato, es decir, si no confirma la medida adoptada y colocada por la policía judicial, ya que la revoca, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso y no podrá ser utilizada. Es cierto que esta consecuencia solamente se contempla expresamente en una medida concreta, la utilización de dispositivos de captación de la imagen, seguimiento y localización en el artículo 588 quinquies b). Pero entendemos que es aplicable a las demás medidas al tener el mismo fundamento, tratarse de medidas inicialmente adoptadas por la policía judicial (o el Ministro o Secretario de Estado en su caso) pero

luego no validadas judicialmente al no cumplir los requisitos para su adopción, no pudiendo valer por ato la información obtenida durante la vigencia de la medida.

En cuanto a si la medida debe comunicarse a la persona afectada –en los casos de adopción policial y no validación judicial posterior- entendemos que sí en virtud de la STEDH caso Roman Zakharov c Rusia de 4 de diciembre de 2015, comentada en la cuestión anterior.

C) DEBATE SOBRE INTERVENCIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS; GRABACIÓN COMUNICACIONES ORALES, CAPTACIÓN DE IMÁGENES; DISPOSITIVOS DE SEGUIMIENTO Y LOCALIZACIÓN.

¿Cabe grabar comunicaciones orales de sospechosos con abogados? ¿en encuentros sexuales? ¿en aseos o lavabos? etc.

Debemos partir necesariamente de la STS 79/2012 en la que se condena a un Magistrado por prevaricación por haber autorizado la grabación de las comunicaciones personales mantenidas entre los imputados presos y sus abogados defensores (respecto de los que no existía indicios de actuación criminal) o con otros letrados que mantuvieran entrevistas con ellos en el centro penitenciario, al haber restringido de manera sustancial el derecho de defensa. Considera la sentencia referida que la confianza y la confidencialidad de las relaciones entre el imputado y su letrado defensor son aspectos esenciales para la efectividad del derecho de defensa. Y *el derecho, para el acusado, de comunicar con su abogado sin ser oído por terceras personas, figura entre las exigencias elementales del proceso equitativo en una sociedad democrática y deriva del artículo 6.3 c) del Convenio. Si un abogado no pudiese entrevistarse con su cliente sin tal vigilancia y recibir de él instrucciones confidenciales, su asistencia perdería mucha de su utilidad*…Además que otros derechos relacionados, como el derecho a no declarar, el derecho al secreto profesional o el derecho a la intimidad, sufrirían reducciones muy sustanciales. Para poder restringir el derecho de acceso de un acusado a su letrado se requiere, entre otros, una previsión legal suficiente, y en nuestra legislación, las comunicaciones entre los internos y sus abogados defensores solamente podían ser intervenidas por orden de la autoridad judicial y en casos de terrorismo. Concluyendo la sentencia referida que *para resolver otros casos en los que se entendiera que la intervención pudiera ser imprescindible, sería precisa una reforma legal que contuviera una habilitación de calidad suficiente para intervenir las comunicaciones entre internos y letrados defensores o expresamente llamados en relación con asuntos penales, estableciendo los casos y las circunstancias en que tal intervención sería posible y las consecuencias de la misma.* Conviene también traer a colación la STEDH Caso Pruteau c. Rumanía de 3 de febrero de 2015 (Pruteau es un abogado de nacionalidad rumana que alega interceptación de las comunicaciones en su teléfono), en la que el

TEDH parte de un pronunciamiento claro y es que las grabaciones de conversaciones entre abogado y su cliente afectan a la confidencialidad, base de la relación de confianza y piedra angular del derecho de defensa, y al secreto profesional y su interceptación y grabación vulnera el art. 8 CEDH, a menos que esté prevista por la ley nacional y persiga uno o más objetivos legítimos en virtud del apartado 2 del citado artículo. Establece la necesidad de examinar si los procedimientos penales para el control de la adopción y aplicación de medidas restrictivas de las comunicaciones entre abogado y cliente son capaces de limitarse a lo estrictamente necesario en una sociedad democrática.

Pues bien, ahora ya tenemos la cobertura legal, ya que el artículo 520.7 Lecrim establece como regla general, que *las comunicaciones entre el investigado o encausado y su abogado tendrán carácter confidencial en los mismos términos y con las mismas excepciones previstas en el apartado 4 del art. 118*, que dispone que *todas las comunicaciones entre el investigado o encausado y su abogado tendrán carácter confidencial. Si estas conversaciones o comunicaciones hubieran sido captadas o intervenidas durante la ejecución de algunas de las diligencias reguladas en esta Ley, el juez ordenará la eliminación de la grabación o la entrega al destinatario de la correspondencia detenida, dejando constancia de estas circunstancias en las actuaciones.* No obstante, y ya introduce como excepción, la posibilidad de su interceptación, *cuando se constate la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal, sin perjuicio de lo dispuesto en la Ley General Penitenciaria.* Por lo que si concurren todos los presupuestos previstos en el art. 588 bis Lecrim: especialidad, idoneidad, excepcionalidad necesidad y proporcionalidad, tras efectuar la ponderación de los intereses en conflicto y afectados, y existieran indicios racionales de criminalidad también contra el abogado, se podría autorizar esta medida. Por otra parte, ya no se limita únicamente a los supuestos de terrorismo, sino también es aplicable a delitos dolosos con pena con límite máximo de al menos 3 años, y delitos cometidos en el seno de un grupo u organización criminal (588 ter a) y quáter b), previa la concurrencia de los siguientes presupuestos:

- indicios objetivos de la participación del abogado en el hecho delictivo investigado (que ha de ser los ya referidos) o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal,

Y si se tratara de grabación de comunicaciones orales, a tenor de lo dispuesto en el artículo 588 quáter b y e, estaría limitada a uno o varios encuentros concretos, cesando la medida cuando estos encuentros terminen. Y si fuera necesario grabar las conversaciones en otros encuentros, será precisa una nueva autorización judicial.

Por otra parte y en cuanto a la posibilidad de grabar comunicaciones orales de sospechosos en encuentros sexuales o lavabos, el artículo 588 quáter a), permite la colocación y grabación de las comunicaciones orales directas del investigado en los siguientes lugares:

- la vía pública,
- cualquier otro espacio abierto,
- domicilio del investigado,
- cualquier otro lugar cerrado

Por lo que en principio pocos espacios hay excluidos de dicha posibilidad, aunque lógicamente se exigiría una motivación especialmente reforzada en determinados ámbitos de ejercicio de privacidad intensa donde se desarrollen actividades íntimas.

Resulta curioso el Auto del Tribunal Supremo de 10 de junio de 2013, resolviendo en una causa especial el recurso de apelación contra el auto de archivo de las actuaciones contra una magistrada por prevaricación judicial. La magistrada había autorizado la grabación sonora de la comunicación vis a vis que la persona investigada iba a tener con su pareja sentimental en el centro penitenciario porque había indicios de posibles confidencias en dicho encuentro. Y el Tribunal Supremo confirma el archivo sobre la base (cuestionable) de que ningún derecho fundamental tiene por sí mismo el carácter de absoluto e ilimitado y que la medida autorizada podría ser necesaria, idónea y proporcionada de cara a la investigación penal. Por lo que la decisión de acceder a la grabación del encuentro la considera estimable, ya que la finalidad del sacrificio del derecho a la intimidad está justificada ante la necesidad de avanzar en la investigación de hechos delictivos de evidente gravedad, si bien adoptándose la excusión y el borrado de determinados minutos por la carencia de interés.

¿Cabe instalar escuchas orales en el domicilio de un tercero no investigado?

En esta cuestión no hemos alcanzado unanimidad en el seminario. La mayoría no considera autorizable la instalación de dispositivos electrónicos aptos captar y grabar las comunicaciones orales mantenidas en el domicilio de una tercera persona no investigada, y ello por considerar que si no está investigada y tampoco resulta ninguna imputación con posterioridad a la medida, no estaría justificada la injerencia en el derecho fundamental a la intimidad e inviolabilidad del domicilio. De hecho, el artículo 588 quáter a solamente habla del domicilio del investigado, no pudiendo extender la mención de “otro lugar cerrado” al domicilio de una tercera persona no investigada. Sin embargo, también hay quien consideraba que en supuestos excepcionales y valorando la proporcionalidad se podría autorizar, por ejemplo, si hubiera indicios de que las personas implicadas en la organización criminal se van a reunir en el domicilio de un tercero para preparar su próximo envío de drogas.

¿Puede la Policía motu propio auxiliar a un particular para grabar la conversación de un tercero?

En diversas demandas examinadas por el TEDH (SSTEDH A. c. Francia, de 23 de noviembre de 1993; M.M. v. Holanda, 8/04/2003; o Bykov v. Rusia, 10/03/2009), la Policía se coordinó con un particular para la recogida de pruebas mediante la grabación de las conversaciones con el sospechoso.

El TEDH concluye en dichos supuestos la existencia de vulneración del art. 8 CEDH y para ello realiza una neta diferenciación entre los supuestos en los que los ciudadanos, directamente, sin auxilio de la policía, realiza ese tipo de grabaciones, frente a los supuestos examinados en los que la Policía pretende reunir pruebas para un proceso penal, y pone a disposición del particular los medios de grabación y controla la obtención de las pruebas preordenadas al proceso penal, en cuyo caso debe solicitar autorización judicial.

La contribución crucial de la policía para reunir pruebas, considera el TEDH, determina una injerencia de la autoridad pública, que debe ser sometida a los mismos requisitos que las intervenciones telefónicas.

Lo contrario, según sostiene el TEDH, equivaldría a permitir que las autoridades investigadoras eludan sus obligaciones derivadas del CEDH mediante el uso de agentes privados.

¿Se pueden colocar y utilizar dispositivos electrónicos de escucha y grabación en una celda?

Resulta útil partir de la STC 145/2014 que declaró la vulneración del derecho fundamental al secreto de las comunicaciones por las grabaciones efectuadas en dependencias policiales. En el caso examinado, se había autorizado, mediante la colocación de micrófonos, la grabación de las conversaciones verbales de las personas detenidas mantenidas en los calabozos policiales. Esta medida se adoptó bajo la cobertura legal del artículo 579.2 Lecrim. El Tribunal Constitucional explicaba que *toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, una habilitación legal* porque constituye "el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas". Y que dicha ley habilitadora de las injerencias debe "definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad". Concluyó que ni el artículo 579.2 de la Ley de enjuiciamiento criminal ni tampoco la normativa penitenciaria, habilitan la intervención de las comunicaciones verbales directas entre los detenidos en dependencias policiales. Aclarando que no estamos ante un defecto por insuficiencia de la ley, sino ante una

ausencia total y completa de ley. Y resulta interesante la STEDH caso Wisse c. Francia de 20 de diciembre de 2005, en el que se intervinieron las escuchas a los internos en el centro penitenciario durante el régimen de visitas de familiares, tomando como parámetro la expectativa razonable de privacidad y estableciendo conforme al mismo la frontera de la intimidad de la vida privada garantizada por el artículo 8 del Convenio en la distinción entre la vigilancia de los actos de una persona en un lugar público por seguridad, de las grabaciones de dichos actos que pueden ser utilizadas con otros fines que van más allá de los que el interesado haya podido prever. Concluyendo que la escucha por la Administración penitenciaria de las conversaciones mantenidas en el locutorio efectuadas por razones de seguridad es perfectamente legítima, no ocurre lo mismo con la grabación sistemática de éstas con otros fines que se incluyen en las nociones de vida privada y de correspondencia, constituyendo una evidente injerencia en la vida privada, vulnerando abiertamente el derecho a la intimidad.

Por tanto, ahora hay cobertura legal pero con los presupuestos referidos y tras el adecuado juicio de proporcionalidad ponderando los derechos en conflicto.

¿Cabe instalar aparatos de escucha en un domicilio consintiendo el acceso el comorador en caso de contraposición de intereses con el investigado?

Conviene comenzar recordando la conexión que nuestra jurisprudencia establece entre la inviolabilidad domiciliaria y el derecho a la intimidad. Desde la STC 22/1984, de 17 de febrero, FJ 2, se viene afirmando que la protección constitucional del domicilio es "una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona".

Fuera de los casos de flagrante delito, sólo son constitucionalmente legítimos la entrada o el registro efectuados con consentimiento de su titular o al amparo de una resolución judicial (SSTC 22/1984, de 17 de febrero, FFJJ 3 y 5; 10/2002, de 17 de enero, FJ 5. Lo que se garantiza, ante todo, es la facultad del titular de excluir a otros de ese ámbito espacial reservado, de impedir o prohibir la entrada o la permanencia en él de cualquier persona y, específicamente, de la autoridad pública para la práctica de un registro.

En la STC 22/2003 (caso Magadán) se analizó un supuesto en el que la esposa prestó consentimiento para la práctica de un registro en un caso en el que la actuación policial se produjo ante un delito flagrante de amenazas, puesto que los dos policías que inicialmente acudieron al citado domicilio lo hicieron ante la llamada de una mujer, a la que el recurrente (su marido) estaba amenazando con un arma de fuego en el interior del domicilio conyugal, y oyeron personalmente los disparos, quedando legitimada en ese momento la entrada en el domicilio por la flagrancia del delito, pero que posteriormente, habiendo sido traslado el recurrente

detenido, una segunda unidad policial accedió a la vivienda con el consentimiento de la mujer. El análisis constitucional que realiza la citada STC 22/2003 se centró en la determinación de quién puede consentir una entrada y registro policial, a los efectos del citado art. 18.2, en los supuestos de cotitulares del domicilio de igual derecho y, en concreto, en los casos de convivencia conyugal o análoga.

Expuso el TC que la convivencia presupone una relación de confianza recíproca, que implica la aceptación de que aquél con quien se convive pueda llevar a cabo actuaciones respecto del domicilio común, del que es cotitular, que deben asumir todos cuantos habitan en él y que en modo alguno determinan la lesión del derecho a la inviolabilidad del domicilio. En definitiva, esa convivencia determinará de suyo ciertas modulaciones o limitaciones respecto de las posibilidades de actuación frente a terceros en el domicilio que se comparte, derivadas precisamente de la existencia de una pluralidad de derechos sobre él.

Como regla general afirma el TC que en una situación de convivencia normal, en la cual se actúa conforme a las premisas en que se basa la relación, y en ausencia de conflicto, cada uno de los cónyuges o miembros de una pareja de hecho está legitimado para prestar el consentimiento respecto de la entrada de un tercero en el domicilio, sin que sea necesario recabar el del otro, pues la convivencia implica la aceptación de entradas consentidas por otros convivientes.

De modo que, aunque la inviolabilidad domiciliaria, como derecho, corresponde individualmente a cada uno de los que moran en el domicilio, la titularidad para autorizar la entrada o registro se atribuye, en principio, a cualquiera de los titulares del domicilio.

Sin embargo, expone a continuación el TC, que el consentimiento del titular del domicilio, al que la Constitución se refiere, no puede prestarse válidamente por quien se halla, respecto al titular de la inviolabilidad domiciliaria, en determinadas situaciones de contraposición de intereses que enerven la garantía que dicha inviolabilidad representa, pues si así fuese, no habría, en realidad, garantía alguna, sin que pueda estimarse válido el consentimiento prestado por la esposa que, al ser víctima del delito, tenía intereses contrapuestos a los del recurrente en el proceso penal.

Aunque la esposa era ciertamente cotitular del domicilio, no estaba legitimada para prestar el consentimiento válidamente permitiendo, en un proceso penal instruido por delito del que era víctima, un registro sobre las pertenencias del acusado orientado a la obtención de pruebas incriminatorias contra él, concluyendo la vulneración del derecho del recurrente a la inviolabilidad domiciliaria (art. 18.2 CE). No obstante, el TC aplicó excepcionalmente el estándar de “buena fe” en la actuación policial.

¿Cabe instalar aparatos de escucha en un domicilio tras franquear el acceso el morador pero sin su conocimiento?

Tal y como establece la STC 173/2011, de 7 de noviembre, el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto "*aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida"* (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2). En lo relativo a la forma de prestación del consentimiento, no precisa ser expreso, admitiéndose también un consentimiento tácito (STC 196/2004, de 15 de noviembre), y que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito (STC 209/2007, de 24 de septiembre).

En el mismo sentido, la STC 173/2011, expone que el derecho a la intimidad personal se vulnera también cuando, aun autorizada su intromisión en un primer momento, se subvierten después los términos y el alcance para el que se otorgó.

¿Qué valor probatorio cabe reconocer a las imágenes con cámara oculta en dependencias privadas, consultas profesionales, vía pública, etc.?

Partimos de la STS 793/2013 dictada en el conocido caso de los abortos practicados en varias clínicas de Barcelona, que se inició por la cámara oculta de dos periodistas suecos. Al respecto, dicha sentencia recoge la doctrina constitucional que ha fijado importantes *limitaciones al uso de la cámara oculta como medio de obtención inconsentida de imágenes y sonidos que luego son objeto de difusión en algún medio de comunicación.* Y que considera que el espacio físico en el que una persona desarrolla su actividad profesional forma parte del contenido material de los derechos a la intimidad y a la propia imagen, *en la medida en que puede existir una razonable expectativa de intimidad,* al poder desarrollarse en dicho ámbito del trabajo o la profesión *relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada.* Sin embargo, matiza el Tribunal Supremo, no hay una prohibición absoluta y excluyente de un determinado medio de prueba en el proceso penal. Así, el Tribunal Constitucional, ante el conflicto entre el derecho a la intimidad y el derecho a la libre difusión de información, se muestra favorable a la prevalencia de aquel, ya que *la utilización de un mecanismo técnico de grabación de la imagen y del sonido, para su ulterior difusión en un medio de comunicación, puede*

entrañar una irreparable lesión de derechos personalísimos del entrevistado que, desconocedor de que su imagen y sus palabras están siendo grabadas clandestinamente, llega a conducirse con un grado de espontaneidad que no ofrecería si conociera el verdadero propósito que anima a su interlocutor. El desconocimiento de la persona que está siendo grabada le impide ejercer su legítimo poder de exclusión frente a dicha grabación, por lo que la ausencia de *conocimiento y, por tanto, de consentimiento de la persona fotografiada respecto a la intromisión en su vida privada es un factor decisivo en la necesaria ponderación de los derechos en conflicto*. De ahí que el Tribunal Constitucional, en sintonía con la jurisprudencia del TEDH, en el juicio de ponderación de los derechos en conflicto y en el momento de decidir cuál de ellos ha de ser sacrificado, opte por desplazar el derecho a la información frente a los derechos a la intimidad y a la propia imagen del afectado. Sin embargo, cuando el conflicto lo es con otros derechos que concurren en el proceso penal, no siempre debe prevalecer el derecho a la imagen y a la intimidad, ya que puede existir un fin legítimo, atendiendo siempre a los principios de proporcionalidad, necesidad y racionalidad.

Por otra parte, la nueva regulación contenida en el artículo 588 quinquies a) permite ahora la utilización de cámaras videográficas por las fuerzas y cuerpos de seguridad del Estado, que les permite obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público. Y las imágenes captadas constituyen un medio válido de prueba evidentemente si son autenticas y no están manipuladas. Con la nueva regulación se pueden grabar imágenes de la persona investigada en lugares públicos:

- si es necesario para facilitar su identificación,
- o localización de los instrumentos o efectos del delito,
- o para obtener datos relevantes para el esclarecimiento de los hechos.

La medida puede afectar a personas diferentes del investigado siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación. No se establece limitación temporal a diferencia de lo que contemplaba el Anteproyecto de 2011, en sus artículos 14 y ss. En dichos preceptos establecía que no se pudiera hacer una vigilancia sistemática (más de 5 días consecutivos o más de 5 no consecutivos pero en un mismo mes) y que no se pudieran obtener imágenes sin autorización. Y regulaba expresamente la posibilidad de vigilancia sistemática y la obtención de imágenes, sólo respecto de la persona investigada y respecto a terceros si están relacionados con el investigado o si la medida es necesaria, con la necesaria autorización previa (del fiscal en dicho texto).

En cuanto a la grabación de la conversación por uno de los interlocutores, la STS 421/2014 considera que quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera 'íntima' del interlocutor, pudiesen constituir

atentados al derecho garantizado en el art. 18.1 CE . Otro tanto cabe decir respecto de la grabación por uno de los interlocutores de la conversación telefónica. El acto de la grabación por uno de los interlocutores de la conversación no conculca secreto alguno impuesto por el art. 18.3 y tan sólo, acaso, podría concebirse como conducta preparatoria para la ulterior difusión de lo grabado. Para que la divulgación a terceros del contenido de la grabación pudiera vulnerar el derecho a la intimidad, sería preciso que la conversación tuviera un contenido que afectara al núcleo esencial del derecho a la intimidad, ya sea en su ámbito personal o en el familiar.

Finalmente, en cuanto al tema de detectives privados, debemos traer a colación la STEDH Vuckota-Bojic c. Suiza de 18 de octubre de 2016. Parte del parámetro de la expectativa razonable de privacidad y que la legislación nacional, en el caso examinado, no permitía que la persona asegurada pudiera imaginar o prever que su obligación de proporcionar información comprendiera el derecho a la compañía aseguradora de grabar de imágenes o videos de ella. Y la falta de claridad de la legislación nacional –posibilidad de estas medidas, duración, uso de los datos obtenidos, destrucción de los mismos…- implica la ausencia de garantías efectivas frente al abuso, considerando violación del artículo 8 Convenio.

¿Qué salvaguardas deben establecerse desde el prisma de la proporcionalidad?

Las escuchas orales, con o sin captación de imágenes, constituye uno de los métodos de investigación más invasivos, de ahí que su regulación legal sea sumamente restrictiva en su diseño, restringiéndolas a encuentros concretos, exigiendo también mención concreta del lugar o dependencias que han ser sometidas a vigilancia (art. 588 quater c).

Tomando en cuenta que en dichos lugares cerrados se desarrolla habitualmente el núcleo duro de la intimidad (por ejemplo, cuarto de baño, dormitorio conyugal, etc), otros ordenamientos jurídicos (como por ejemplo, el Código Procesal Alemán) establecen especiales cautelas ordenando el borrado inmediato de conversaciones que afecten al núcleo duro de la privacidad, o documentando, como por ejemplo en Francia, solamente aquellas imágenes o conservaciones que sean de trascendencia.

De ahí el especial cuidado con que la resolución judicial deberá abordar el alcance de la medida, o las dependencias en las que se realice la observación, por exigencias del principio de proporcionalidad, y así mismo, deberán adoptarse especiales cautelas respecto al tratamiento de la copia que contenga las grabaciones e imágenes, pues difícilmente resistirá la regla de proporcionalidad el acceso de otras partes a aspectos íntimos no necesarios para la investigación.

¿Cabe la observación mediante "drones" de espacios al aire libre dentro de propiedades particulares?

Aunque no conocemos supuestos concretos en que se haya planteado la validez de las observaciones realizadas mediante drones, entendemos plenamente trasvasable a este tipo de observaciones visuales y/o acústicas a distancia, la doctrina sentada por la STS nº 329/2016, de 20 de abril, que declara la nulidad de una observación policial, sin orden judicial, de un domicilio realizada a distancia, mediante unos prismáticos y a través de una ventana.

La intromisión virtual supone una injerencia en el domicilio, sin llegar a acceder a su interior, que permite observar o escuchar lo que allí acaece sin el consentimiento de sus titulares. Se caracteriza, a diferencia de la irrupción material y/o personal en el domicilio, por no existir un contacto directo con el domicilio, aunque se accede igualmente al entorno familiar constitucionalmente protegido, y además de un modo imperceptible para los investigados.

La intromisión virtual puede producirse a simple vista u oído, por la ausencia de ventanas, cortinas o cualquier otro elemento de protección que contribuyen a delimitar el espacio íntimo de protección en el que se desarrolla la vida personal y familiar, o también mediante el uso de artilugios, teleobjetivos fotográficos, dispositivos direccionales de grabación de sonido, prismáticos, telescopios o también drones provistos de aparatos de captación de imágenes y sonido.

El ámbito de intimidad protegida viene en cierta medida delimitado por los actos propios que realice el propio individuo, al exteriorizar o permitir que, en mayor o menor medida, terceros ajenos accedan a su intimidad personal y/o familiar, en cuanto no puede calificarse de intromisión ilegítima aquello que oye o ve un policía o cualquier testigo proveniente de un domicilio o conversación desprotegida del escrutinio ajeno (falta de cortinas, conversación en voz alta, etc..).

En consecuencia si un policía, o cualquier testigo, pasa por una calle y observa directamente (sin mayor artificio, esfuerzo o actividad adicional) cómo en el interior de una vivienda se comete un delito, la intromisión no podrá ser calificada de ilícita y la prueba que se derive de la observación será válida.

Ahora bien, ¿hasta qué punto resultaría exigible al ciudadano una acción especialmente exhaustiva dirigida a la protección de su intimidad domiciliaria?

En la STS de 20 de abril de 2016 a la que ya nos hemos referido, se analiza la intromisión que, mediante prismáticos, tuvo como objeto un domicilio sito en una planta 10ª, sin cortinas, desde un edificio cercano, considerando el TS que la intromisión virtual en un domicilio no puede quedar amparado cuando se utilizan

medios tecnológicos como los prismáticos que permiten observar la intimidad domiciliaria sin que los habitantes de la vivienda sean conscientes de ello.

Anteriores sentencias del TS (SSTS 15/04/1997, 18/02/1999) ampararon la intromisión virtual por parte de la policía ante la ausencia de obstáculos físicos (ventanas, cortinas o similares) que la impidieran, aunque bien es cierto, sin el empleo de medios tecnológicos de visión o escucha.

En este sentido, la STS 15/04/1997 declaró que : *«... en lo concerniente a si la observación realizada a través de una ventana requiere autorización judicial, la Sala estima que la respuesta también debe ser negativa. En efecto, en principio, la autorización judicial siempre será necesaria cuando sea imprescindible vencer un obstáculo que haya sido predispuesto para salvaguardar la intimidad. Cuando, por el contrario, tal obstáculo no existe, como en el caso de una ventana que permite ver la vida que se desarrolla en el interior de un domicilio no es necesaria una autorización judicial para ver lo que el titular de la vivienda no quiere ocultar a los demás».* En el mismo sentido en relación a un patio anexo a una vivienda, la STS 18 febrero 1999.

Con cita de ambos precedentes, la STS de 20/04/2016 declara que no puede aceptarse que el derecho a la intimidad en el domicilio reconocido en el art. 18 CE quede al albur del uso por parte de la policía de medios técnicos que sin irrumpir materialmente, lo hacen de forma virtual, lo que así sucedió en el caso examinado, pero que también podría producirse mediante el empleo de otros artilugios de grabación del sonido o drones, lo que no debe depender de que el morador corra una cortina o cierra una ventana.

Así lo entiende el Tribunal Supremo cuando afirma: *«… cuando los agentes utilizan instrumentos ópticos que convierten la lejanía en proximidad, no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior. El domicilio como recinto constitucionalmente protegido no deja de ser domicilio cuando las cortinas no se hallan debidamente cerradas. La expectativa de intimidad, en fin, no desaparece por el hecho de que el titular o usuario de la vivienda no refuerce los elementos de exclusión asociados a cualquier inmueble. Interpretar que unas persianas no bajadas o unas cortinas no corridas por el morador transmiten una autorización implícita para la observación del interior del inmueble, encierra el riesgo de debilitar de forma irreparable el contenido material del derecho a la inviolabilidad domiciliaria…».*

Añade que no puede aceptarse la teoría de los actos propios de dejación del derecho por cuanto: *«la tutela constitucional del derecho proclamado en el apartado 2 del art. 18 CE protege, tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes. El Estado no puede adentrarse sin*

autorización judicial en el espacio de exclusión que cada ciudadano dibuja frente a terceros. Lo proscribe el art. 18.2 CE, y se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un utensilio óptico que permite ampliar las imágenes y salvar la distancia entre el observante y lo observado».

Finalmente, el Tribunal Supremo hace también referencia en su sentencia a la expresa prohibición que establece la LO 4/1997, que regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos, y que en su art. 6.5 dispone que: *«no se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial (...), ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodio».*

Precisamente, el artículo 588 quinquies a de la LECRim posibilita la captación de imágenes en lugares o espacios públicos, no respecto a aquellos otros afectos a la intimidad personal y familiar.

De ahí que los supuestos de utilización de artificios técnicos no son los únicos que quedarían constitucionalmente excluidos, sino también otros supuestos, por ejemplo, cuando un policía se encarama a un poste eléctrico para observar a simple vista el domicilio próximo o convence a un vecino para apostarse y observar lo que allí sucede. En dichos supuestos, la prueba así obtenida también debería considerarse ilícita[1], pues supone una inmisión en la intimidad domiciliaria sin que concurra flagrancia, consentimiento u orden judicial.

Precisamente, el TC tiene declarado que la protección constitucional del domicilio en el art. 18.2 CE se concreta en dos reglas distintas. La primera define su "inviolabilidad", que constituye un auténtico derecho fundamental de la persona, establecido como garantía de que el ámbito de privacidad, dentro del espacio limitado que la propia persona elige, resulte "exento de" o "inmune a" cualquier tipo de invasión o agresión exterior de otras personas o de la autoridad pública, incluidas las que puedan realizarse sin penetración física en el mismo, sino por medio de aparatos mecánicos, electrónicos u otros análogos.

También podemos traer a colación el caso Kyllo V. EEUU (2000) en el que la Corte Suprema de EEUU analizó un supuesto en el que existían sospechas de que el demandante Sr. Kyllo se dedicaba al cultivo de marihuana, y para confirmar dichas sospechas se utilizó un dispositivo de escaner de la imagen térmica para determinar si la cantidad de calor que emanaba de la casa era compatible con las

[1] (RICHARD GONZÁLEZ, *Nulidad de la prueba por la intromisión virtual en domicilio. Una breve reflexión sobre la observación policial ilícita de la intimidad personal y familiar, Diario La Ley, Nº 8788*),

lámparas de alta intensidad típicamente utilizadas para el cultivo de marihuana en lugares cerrados. La imagen reveló áreas relativamente calientes en comparación con el resto de la casa. Sobre la base de confidentes, facturas de servicios públicos, y la imagen térmica, un juez federal emitió una orden para registrar la casa de Kyllo. La búsqueda dio resultado positivo comprobando el cultivo de marihuana en el interior de la vivienda. Kyllo fue condenado y el Tribunal de Apelación sostuvo que no podía afirmarse que Kyllo tuviera una expectativa subjetiva de privacidad porque no había hecho ningún intento de ocultar el calor que se escapaba de su casa, e incluso si lo hubiera hecho, no se habría vulnerado ninguna expectativa razonable de privacidad objetiva debido a que la cámara "no exponía los detalles íntimos de la vida de Kyllo, sino amorfas imgánenes de puntos calientes en el techo y la pared exterior".

El Tribunal Supremo, no obstante, se cuestionó si el uso de un dispositivo de ese tipo para captar imágenes térmicas a fin de detectar cantidades relativas de calor que emanaba de una casa privada constituía una búsqueda contraria a la Cuarta Enmienda, decidiendo por 5 votos a 4 que efectivamente se había producido una violación, pues el Gobierno había utilizado un dispositivo que no está a disposición del público en general para explorar los detalles que no habrían sido posibles de conocer sin la intrusión física en la casa, de tal forma que esa vigilancia térmica constituía una "búsqueda" que requería una previa orden judicial. En el voto disidente se afirmaba que esa información era de dominio público, recogía los datos exteriores de la casa, sin invadir ningún ámbito de intimidad constitucionalmente protegido.

La Corte Suprema de EEUU se ha vuelto a pronunciar con posterioridad en este mismo sentido en el caso Florida V. Jardines (11- 564), en el que se abordó el uso de un perro policía entrenado para detectar narcóticos en el porche de una vivienda, en la que nuevamente por 5 votos a 4 declara que situar un perro policía entrenado en el porche de la vivienda de una persona a los efectos de la obtención de pruebas con la que conseguir una orden de registro viola la Cuarta Enmienda. En el voto disidente se afirma que el agente de policía estaba en su derecho de acercarse a la puerta de una casa y llamar, al igual que cualquier otro ciudadano, independientemente de ir acompañado por un perro policía entrenado.

D) DEBATE SOBRE REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO; REGISTROS REMOTOS; AGENTE ENCUBIERTO ONLINE.

¿Cabe acceder al registro de un dispositivo de almacenamiento masivo con el consentimiento del sujeto?

Sí. En principio, la STS 864/2015 dispone que el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, aunque matizando que dicho consentimiento puede ser revocado en cualquier

momento. Asimismo, respecto del alcance del consentimiento, sigue diciendo la sentencia referida que *se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto "aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (SSTC 196/2004, 206/2007 y 70/2009).* Respecto a la formas del consentimiento, no precisa ser expreso admitiéndose también el consentimiento tácito. Se cita la STC 196/2004, *en la que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, y reconocimos no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad.*

Por otra parte, si la persona está detenida, será necesaria la asistencia de su letrado e información precisa y concreta sobre la finalidad y consecuencias del consentimiento así como que tiene derecho a no prestarlo.

¿Está obligado a proporcionar las claves de acceso o ceder la huella digital?

Entendemos que no ya que iría en contra del derecho a la prohibición de la autoincriminación.

¿Qué razones justifican la exigencia de autorización judicial en el registro de dispositivos de almacenamiento masivo?

A diferencia del art. 18.3 CE (secreto de las comunicaciones) que exige necesariamente previa autorización judicial, el art. 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, de modo que el TC ha admitido que, en algunos casos y con la suficiente y precisa habilitación legal, la policía realice legítimamente determinadas prácticas que constituyan una injerencia **LEVE** en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 70/2002, de 3 de abril, FJ 10; 123/2002, de 20 de mayo, FJ 4; 56/2003, de 24 de marzo, FJ 2; 281/2006, de 9 de octubre, FJ 4; y 142/2012, de 2 de julio, FJ 2).

Pero precisamente, al carácter MASIVO de la información almacenada en este tipo de dispositivos, es el que determina la gravedad de la injerencia, que no merece precisamente el calificativo de “LEVE”.

No hay duda de que los datos personales relativos a una persona individualmente considerados (informes de salud (STC 70/2009 y 159/2009), situación económica (STC 233/1999), declaraciones IRPF (STC 47/2001), gastos

(STC 233/205), agenda personal (STC 70/2002), etc., están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros, datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.), no sólo forma parte de este mismo ámbito, sino que además, a través de su observación por los demás, pueden descubrirse aspectos de la esfera más íntima del ser humano, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran un perfil altamente descriptivo de la personalidad de su titular.

De ahí la gravedad de la injerencia que supone el acceso a dispositivos de almacenamiento masivo.

Esta razón es la que llevó a la Corte Suprema de EEUU a declarar -por un contundente 9 votos a 0- en el caso Riley c. California, de 25 de junio de 2014, la necesidad de obtener una orden judicial para acceder a este tipo de dispositivos. Esta sentencia constituye lo que ha venido a denominarse un *landmark rulling*, en un asunto en el que el sujeto fue parado por una infracción de tráfico al llevar las placas de su vehículo caducadas, se procedió al registro del vehículo, donde se hallaron armas, y a la confiscación e inspección del móvil que portaba en su bolsillo. Se encontraron en el dispositivo fotografías, vídeos y expresiones que lo relacionaban con bandas callejeras y con un tiroteo. Y estas pruebas fueron utilizadas posteriormente en un juicio en el que fue condenado por homicidio. Se planteó así hasta qué punto la policía podía llevar a cabo un control de los efectos personales de un individuo sin necesidad de autorización judicial, en concreto, de un Smartphone, lo que podría también extenderse a tabletas u ordenadores portátiles. En el asunto al que nos referimos, la Jueza del Tribunal Supremo, Elena Kagan, dijo de forma muy gráfica que ahora *"la gente lleva toda su vida en sus móviles".*

La Corte Suprema entendió de forma unánime que los teléfonos móviles se diferencian cualitativa y cuantitativamente de otros objetos que pueda poseer un ciudadano en el momento de ser arrestado, y que el registro de los mismos sin una orden judicial es contrario a lo establecido en la Constitución, porque el contenido del móvil y la suma de datos que en el mismo se pueden obtener puede ofrecer tanto o más sobre la vida privada de una persona que el registro de su casa.

No obstante, en nuestro ordenamiento, el art. 588 sexies c) contempla de forma excepcional que la Policía Judicial pueda llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, en caso de urgencia y cuando se aprecie un interés constitucional legítimo que haga imprescindible la medida.

Este aspecto lo analizamos a continuación en la cuestión siguiente.

¿A qué se refiere la frase "interés constitucionalmente legítimo" que utiliza el art. 588 sexies c, apartado 4 para habilitar a la policía judicial el acceso al contenido de un ordenador, de un móvil, sin autorización judicial?

La cuestión entronca con el diferente régimen de garantías recogido en el art. 18 CE, según se trate de una afectación al derecho al secreto de las comunicaciones (art. 18.3 CE) o del derecho a la intimidad personal (art. 18.1 CE).

Siguiendo con la explicación que hemos ofrecido en la cuestión anterior, el art. 588 sexies c) contempla de forma excepcional que la Policía Judicial pueda llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, en los siguientes términos:

> *4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.*

Esta posibilidad ya había sido avalada por nuestro TC en numerosas ocasiones, indicando que:

"En relación a la necesidad de autorización judicial, el criterio general, conforme a nuestra jurisprudencia, es que sólo pueden llevarse a cabo injerencias en el ámbito de este derecho fundamental mediante la preceptiva resolución judicial motivada que se adecue al principio de proporcionalidad (SSTC 207/1996, de 16 de diciembre, FJ 4; 25/2005, de 14 de febrero, FJ 6; y 233/2005, de 26 de septiembre, FJ 4). Esta regla no se aplica, también según nuestra doctrina, en los supuestos en que concurran motivos justificados para la intervención policial inmediata, que ha de respetar también el principio de proporcionalidad. De manera significativa hemos resaltado en la STC 70/2002, de 3 de abril, que "la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial

motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad" [FJ 10 b) 3]. Bien entendido que "la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante y es susceptible de control judicial ex post, al igual que el respeto al principio de proporcionalidad. La constatación ex post de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales" [FJ 10 b) 5]. En esta línea en la STC 206/2007, de 24 de septiembre, FJ 8, afirmábamos que "la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad".

Ahora bien, dicha posibilidad debe encuadrarse en sus precisos términos, a tenor del reciente pronunciamiento del TEDH (Trabajo Rueda c. España, de 30/05/2017) que anula la STC 173/2011 que avaló una actuación policial derivada de la *notitia criminis* proporcionada por el propietario de una tienda de informática, quien se personó en las dependencias policiales informando acerca del material pedófilo que había encontrado en un ordenador personal que había sido depositado por su dueño con fines de reparación. Con esta actuación, los agentes pretendieron, con la conveniente celeridad que requerían las circunstancias –según explicó el TC-, comprobar la veracidad de lo ya descubierto por este ciudadano, así como constatar si existían elementos suficientes para la detención de la persona denunciada, tomando en consideración que la investigación se refería a un delito de distribución de pornografía infantil. Razonó también el TC que la persona denunciada no estaba detenida cuando se practicó la intervención, *"por lo que tampoco aparece como irrazonable intentar evitar la eventualidad de que mediante una conexión a distancia desde otra ubicación se procediese al borrado de los ficheros ilícitos de ese ordenador o que pudiera tener en la "nube" de Internet. En todo caso, también aparece como un interés digno de reseñar la conveniencia de que por parte de los funcionarios policiales se comprobara con la conveniente premura la posibilidad de que existiesen otros partícipes, máxime en este caso en que se utilizó una aplicación informática que permite el intercambio de archivos, o que, incluso, detrás del material pedófilo descubierto, pudieran esconderse unos abusos a menores que habrían de acreditarse."*

Sin embargo, el TEDH ha anulado recientemente la STC 173/2011 en una importante sentencia de fecha 30/05/2017 (caso Trabajo Rueda c. España), tras demandar, invocando el artículo 8 del CEDH (derecho al respeto a la vida privada y familiar), que la incautación y examen de su ordenador por parte de la policía habían constituido una injerencia en su derecho al respeto de su vida privada y familiar. En efecto, el TEDH precisa que es difícil apreciar, en este caso, la urgencia que habría obligado a la policía a incautarse de los archivos del ordenador personal del Sr. Trabajo Rueda y acceder a su contenido, sin obtener previamente la autorización judicial normalmente requerida, ya que no existía ningún riesgo de desaparición de carpetas y que se trataba de un ordenador incautado y retenido por la policía y no conectado a la red de Internet. El TEDH no logra por tanto detectar las razones por las que la espera de una autorización judicial previa a la intervención en el ordenador del Sr. Trabajo Rueda, que podía obtenerse con relativa rapidez, hubiera obstaculizado la investigación llevada a cabo por la policía de los hechos denunciados. En consecuencia el TEDH concluye que ha habido violación del artículo 8 del Convenio.

En el mismo sentido la sentencia Riley c. California, citada en la cuestión anterior, destacó la exigencia de autoridad judicial, en atención a la gravedad de la injerencia, y a la inexistencia de razones de urgencia, pues las personas detenidas no estaban en disposición de *"eliminar datos incriminatorios".*

¿Qué límites cabe establecer en el registro de dispositivos de almacenamiento masivo?

Como ya se ha dicho, uno de los objetivos de la reforma es precisar con exactitud la medida, alcance o extensión de la injerencia de tal manera que se acceda solamente a la información necesaria para la investigación y por tanto evitar la intrusión innecesaria en toda la esfera de privacidad de la persona afectada con la medida. De esta forma, ya el artículo 588 bis b y c, en el ámbito de las disposiciones generales comunes a todas las medidas de investigación tecnológica, exige que la solicitud de autorización judicial precise expresamente la extensión de la medida con especificación de su conde nido y que el auto autorizando la medida concrete la extensión de la medida de injerencia especificando su alcance. En el ámbito de los registros de dispositivos de almacenamiento masivo de información, el artículo 588 sexies c) exige que la resolución judicial que autorice el acceso a la información contenida en dichos dispositivos fije los términos y el alcance del registro. Como se dice en la exposición de motivos de la Ley, la reforma *"descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido*". Recoge así la jurisprudencia existente al respecto. Así, la STC 173/2011 llamaba la atención sobre la importancia de dispensar protección constitucional al *cúmulo de información personal derivada de los instrumentos tecnológicos de nueva generación y que se almacena por su titular en*

un ordenador o en un móvil Iphone sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.), por lo que a través de la observación de estos dispositivos pueden descubrirse aspectos de la esfera más íntima del ser humano, ya que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Y si bien estos datos. Sigue diciendo el Tribunal Constitucional, considerados aisladamente pueden considerarse de livianos, *si se analizan en su conjunto una vez entremezclados, no cabe duda de que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador, o cualquier dispositivo técnico que lo permita, es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado.* Por ello, dice el TC, *deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información* ".

Y una de estas garantías es acordar la medida en la extensión que resulte estrictamente necesaria para el fin perseguido. Lo contrario no sería proporcional dada la cantidad y calidad de información a la que se accedería, como acabamos de ver, suponiendo una injerencia injustificada que afectaría a varios derechos de su titular. Y no se puede convalidar dicha inherencia, ab initio desproporcionada al no ser necesaria para la investigación del delito en cuestión, a posteriori en virtud del resultado obtenido. Al respecto, como dice la Audiencia Provincial de Tarragona (sentencia 3-11-2003), el juicio de necesidad se vincula de manera esencial con la justificación ex ante. *Lo contrario, es decir, la justificación ex post, sólo por el resultado, de cualquier medio o forma de actuación policial o judicial, equivaldría a la pura y simple derogación del art. 11.1 Ley Orgánica Poder Judicial e, incluso, de una parte, si no de todo, del artículo 24 CE, sin olvidar, me atrevería a añadir, el propio contenido reaccional y esencial del derecho fundamental sustantivo que se vería afectado*. *Esta necesaria, por insoslayable, perspectiva metodológica ex ante en el análisis de los gravámenes de constitucionalidad por lesión derechos fundamentales sustantivos en la práctica de diligencias injerentes también ha sido destacada por el Tribunal Constitucional en su STC 136/2000 ["en la revisión de la proporcionalidad de la medida este Tribunal no ha de tomar en consideración ninguna circunstancia habida*

con posterioridad al momento en que se adoptó la medida restrictiva del derecho fundamental"].

El letrado de la defensa comunica que en el ordenador del investigado se encuentra información enmarcada en la relación cliente-letrado que afecta al derecho de defensa, ¿cómo debemos proceder?

En su sentencia de 3 de febrero de 2015, en el asunto Pruteanu vs. Rumanía, el Tribunal Europeo de Derechos Humanos (TEDH) ampara en su derecho al demandante y considera que la interceptación de conversaciones entre abogado y cliente afecta directamente a la confidencialidad, que es la base de la relación de confianza y del derecho de defensa.

De ahí que el art. 118.4 LECRim recoja expresamente que todas las comunicaciones entre el investigado o encausado y su abogado tendrán carácter confidencial. Si estas conversaciones o comunicaciones hubieran sido captadas o intervenidas durante la ejecución de alguna de las diligencias reguladas en esta ley, el juez ordenará la eliminación de la grabación o la entrega al destinatario de la correspondencia detenida, dejando constancia de estas circunstancias en las actuaciones.

Lo dispuesto en el párrafo anterior no será de aplicación cuando se constate la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal, sin perjuicio de lo dispuesto en la Ley General Penitenciaria.

La STS de 9/02/2012 (ponente Sr. Colmenero) recordó, en este mismo sentido, que la confidencialidad de las relaciones entre el imputado y su letrado defensor, que naturalmente habrán de estar presididas por la confianza, resulta un elemento esencial (STEDH Castravet contra Moldavia, de 13 de marzo de 2007, p. 49; y STEDH Foxley contra Reino Unido, de 20 de junio de 2000, p. 43). En la STEDH de 5 de octubre de 2006, caso Viola contra Italia (61), se decía que *"...el derecho, para el acusado, de comunicar con su abogado sin ser oído por terceras personas figura entre las exigencias elementales del proceso equitativo en una sociedad democrática y deriva del artículo 6.3 c) del Convenio. Si un abogado no pudiese entrevistarse con su cliente sin tal vigilancia y recibir de él instrucciones confidenciales, su asistencia perdería mucha de su utilidad (Sentencia S. contra Suiza de 2 noviembre 1991, serie A núm. 220, pg. 16, ap. 48). La importancia de la confidencialidad de las entrevistas entre el acusado y sus abogados para los derechos de la defensa ha sido afirmada en varios textos internacionales, incluidos los textos europeos (Sentencia Brenan contra Reino Unido, núm. 39846/1998, aps. 38-40, TEDH 2001-X)".*

En este mismo sentido, el Tribunal de Justicia de las Comunidades Europeas en la Sentencia (Gran Sala) de 14 de setiembre de 2010, señaló que *"la confidencialidad de las comunicaciones entre los abogados y sus clientes debía ser objeto de protección a nivel comunitario", aunque supeditó tal beneficio a dos requisitos: "...por una parte, debe tratarse de correspondencia vinculada al ejercicio de los derechos de la defensa del cliente, y, por otra parte, debe tratarse de abogados independientes, es decir, no vinculados a su cliente mediante una relación laboral".*

En el desarrollo de la comunicación entre letrado y cliente, basada en la confianza y en la seguridad de la confidencialidad, y con mayor razón en el ámbito penal, es lo natural que aparezcan valoraciones sobre lo sucedido según la versión del imputado, sobre la imputación, sobre las pruebas existentes y las que podrían contrarrestar su significado inculpatorio, sobre estrategias de defensa, e incluso podría producirse una confesión o reconocimiento del imputado respecto de la realidad de su participación, u otros datos relacionados con la misma. Es fácil entender que, si los responsables de la investigación conocen o pueden conocer el contenido de estas conversaciones, la defensa pierde la mayor parte de su posible eficacia. En la primera de las sentencias antes citadas, Castravet contra Moldavia, el TEDH afirmó en este sentido que *"...si un abogado no fuera capaz de departir con su cliente y recibir instrucciones de él sin supervisión, su asistencia perdería gran parte de su utilidad, teniendo en cuenta que el Convenio pretende garantizar derechos prácticos y efectivos"*

No es preciso, por lo tanto, que aparezca un aprovechamiento expreso mediante una acción concreta y directamente relacionada con lo indebidamente sabido, pues basta para lesionar el derecho de defensa con la ventaja que supone para el investigador la posibilidad de saber, (y con mayor razón el conocimiento efectivo), si el imputado ha participado o no en el hecho del que se le acusa, saber si una línea de investigación es acertada o resulta poco útil, saber cuál es la estrategia defensiva, cuales son las pruebas contrarias a las de cargo, o incluso conocer las impresiones, las necesidades o las preocupaciones del imputado, o los consejos y sugerencias que le hace su letrado defensor. Se trata de aprovechamientos más sutiles, pero no por eso inexistentes. Basta, pues, con la escucha, ya que desde ese momento se violenta la confidencialidad, elemento esencial de la defensa.

El TEDH ha señalado en este sentido que la injerencia existe desde la interceptación de las comunicaciones, sin que importe la posterior utilización de las grabaciones (STEDH Kopp contra Suiza, de 25 de marzo de 1998).

Además, sufrirían reducciones muy sustanciales otros derechos relacionados. En primer lugar, el derecho a no declarar. La comunicación con el letrado defensor se desarrolla en la creencia de que está protegida por la

confidencialidad, de manera que en ese marco es posible que el imputado, solo con finalidad de orientar su defensa, traslade al letrado aspectos de su conducta, hasta llegar incluso al reconocimiento del hecho, que puedan resultar relevantes en relación con la investigación. Es claro que el conocimiento de tales aspectos supone la obtención indebida de información inculpatoria por encima del derecho a guardar silencio. En estos casos, la prohibición de valoración de lo ya conocido no es más que un remedio parcial para aquellos casos en los que, justificada la intervención con otros fines, el acceso haya sido accidental e inevitable, pero de esa forma no se elimina la lesión ya causada en la integridad del derecho.

En segundo lugar, el derecho al secreto profesional. Concebido como un derecho del letrado a no revelar los datos, de la clase que sean, proporcionados por su cliente, o, con carácter más general, obtenidos en el ejercicio del derecho de defensa (artículo 416 de la LECrim y 542.3 de la LOPJ), opera también como un derecho del imputado a que su letrado no los revele a terceros, ni siquiera bajo presión. El conocimiento indebido del contenido de las comunicaciones entre ambos, pues, dejaría en nada este derecho.

En tercer lugar, el derecho a la intimidad. La relación entre el imputado y su letrado defensor se basa en la confianza, de forma que es altamente probable que estando el primero privado de libertad traslade al segundo cuestiones, observaciones o preocupaciones que excedan del derecho de defensa para residenciarse más correctamente en el ámbito de la privacidad, que solo puede ser invadido por el poder público con una razón suficiente.

No se trata, por otra parte, de derechos absolutos. El TEDH, en la Sentencia Viola contra Italia, de 5 de octubre de 2006 , señaló que *"...el acceso de un acusado a su abogado puede estar sometido a restricciones por razones válidas. Se trata de saber en cada caso si, a la luz del conjunto del procedimiento, la restricción privó al acusado de un proceso equitativo".*

Pero sus posibles restricciones, que no siempre son aceptables en la misma medida, requieren, según la interpretación que el TC ha hecho de la Constitución y el TEDH del Convenio, del cumplimiento suficiente de, al menos, tres exigencias. En primer lugar, una previsión legal suficiente, (en este sentido, STC 196/1987 y otras muchas), que en nuestro ordenamiento, en tanto que ley de desarrollo de un derecho fundamental, debe respetar en todo caso su contenido esencial (artículo 53.1 CE). En segundo lugar, una justificación suficiente en el supuesto concreto, que tenga en cuenta los indicios disponibles en el caso, la necesidad de la medida y el respeto al principio de proporcionalidad. A este aspecto se refieren la STEDH de 2 noviembre 1991 Caso S. contra Suiza y la STEDH de 31 enero 2002 Lanz contra Austria. Y en tercer lugar, en nuestro Derecho, una autorización judicial, regulada en ocasiones de forma expresa y en otras de forma implícita, según ha establecido el TC, aunque su forma y características admitan algunas matizaciones en función de la entidad de la restricción.

Naturalmente, todas estas consideraciones no pueden entenderse referidas solo a los efectos que producen en el caso concreto las escuchas de las comunicaciones reservadas entre el imputado y su letrado defensor. De aceptarse que la mera posibilidad de que se sigan cometiendo delitos justifica la supresión de la confidencialidad entre el imputado preso y su letrado defensor, desaparecería de manera general un elemento esencial en la misma configuración del proceso justo. Incluso la mera sospecha fundada acerca de la existencia de escuchas generalizadas de las comunicaciones entre el imputado privado de libertad y su letrado defensor, anularía de manera general la confianza en una defensa con capacidad de efectividad, como elemento imprescindible para un proceso con igualdad de armas; un proceso, por tanto, equitativo. En este sentido, en la STEDH Castravet contra Moldavia, de 13 de marzo de 2007 , antes citada, ya se advirtió que *"...una injerencia en el privilegio abogado-cliente, y por ende, en el derecho del detenido a la defensa, no exige necesariamente que tenga lugar una intercepción real o una escucha subrepticia. Una creencia genuina, basada en indicios razonables de que su conversación está siendo escuchada, puede ser suficiente, desde el punto de vista del Tribunal, para limitar la efectividad de la asistencia que el abogado pueda proporcionar. Tal creencia inhibiría inevitablemente la libertad de discusión entre el abogado y el cliente, y vulneraría el derecho del detenido a rebatir de forma efectiva la legalidad de su detención".*

Se han traído a colación los casos en los que se intervienen comunicaciones de un sospechoso y entre las que son grabadas aparecen algunas con su letrado defensor, o aquellos otros en los que existiendo indicios de actuación criminal contra un letrado o letrados, se intervienen sus comunicaciones personales o las de sus despachos, y entre las conversaciones mantenidas aparecen algunas con sus clientes relativas al ejercicio del derecho de defensa. A estas se ha referido en alguna ocasión la jurisprudencia de la Sala 2ª. Así, en la STS nº 2026/2001, FJ 9, en la que se decía que *"El secreto profesional que protege a las relaciones de los abogados con sus clientes, puede, en circunstancias excepcionales, ser interferido por decisiones judiciales que acuerden la intervención telefónica de los aparatos instalados en sus despachos profesionales. Es evidente que la medida reviste una incuestionable gravedad y tiene que ser ponderada cuidadosamente por el órgano judicial que la acuerda, debiendo limitarse a aquellos supuestos en los que existe una constancia, suficientemente contrastada, de que el abogado ha podido desbordar sus obligaciones y responsabilidades profesionales integrándose en la actividad delictiva, como uno de sus elementos componentes".*

¿Deben entenderse incluidos los datos relativos a las llamadas telefónicas u otras comunicaciones, si nada expresa la autorización judicial –art. 588 sexies c).4-?

Entendemos que la respuesta negativa, salvo previsión expresa en el auto autorizante, vendría basada en el mismo fundamento en que se basa la previsión legal expresa contenida en el art. 588 sexies a) párrafo 2º, en la que se aclara que la autorización para entrada y registro en la que se incaute cualquier dispositivo de almacenamiento masivo de información, no legitima el acceso su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

De forma análoga, la autorización de acceso al contenido un aparato de almacenamiento masivo, deberá especificar expresamente si este acceso va referido también a los datos relativos a las llamadas telefónicas u otras comunicaciones que consten en este dispositivo.

La versatilidad tecnológica que han alcanzado los dispositivos de almacenamiento masivo (teléfonos móviles, tablets, smartphones, etc) convierte a estos terminales en herramientas habituales en la vida cotidiana con múltiples funciones, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.), susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo al derecho a la intimidad, sino también al secreto de las comunicaciones (art. 18.3 CE), lo que implica que el parámetro de control a proyectar deba ser especialmente riguroso (STC de Pleno 115/2013, de 9 de mayo), tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la ley, como desde la perspectiva de si la concreta actuación desarrollada al amparo de la ley se ha ejecutado respetando escrupulosamente el principio de proporcionalidad.

De ahí que nuestro TC a la hora de enfrentarse a esta materia, fundamentalmente en los supuestos de acceso policial limitado a los datos recogidos en el archivo electrónico o **agenda** de contactos telefónicos de un terminal móvil —sin afectar al registro de llamadas entrantes y salientes, ni a ningún otro archivo o enlace que pudiera contener el terminal móvil— ha declarado que el acceso limitado practicado en esos precisos términos constituye una injerencia en el derecho a la intimidad personal (art. 18.1 CE), al igual que lo es la apertura de una **agenda** en soporte de papel y la lectura de los papeles encontrados en ella (STC 70/2002, FJ 9), que recoge una relación de números telefónicos identificados habitualmente mediante un nombre.

Muy diferente de aquellos supuestos en los que se accede a información relativa al registro de llamadas, en cuyo caso el TC ha reiterado (entre otras, SSTC

281/2006, de 9 de octubre, FJ 4; 230/2007, de 5 de noviembre, FJ 2; 142/2012, de 2 de julio, FJ 3 y 241/2012, de 17 de diciembre, FJ 4) que el derecho al secreto de las comunicaciones (art. 18.3 CE) consagra tanto la interdicción de la interceptación como el conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado no sólo por la interceptación en sentido estricto —aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación— sino también por el conocimiento antijurídico de lo comunicado, como puede suceder, sin ánimo de exhaustividad, en los casos de apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil. Igualmente se ha destacado que el derecho al secreto de las comunicaciones protege no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores, por lo que queda afectado por este derecho tanto la entrega de los listados de llamadas telefónicas por las compañías telefónicas como el acceso al registro de llamadas entrantes y salientes grabadas en un **teléfono móvil** (por todas, SSTC 123/2002, FJ 6; 56/2003, FJ 3; 230/2007, FJ 2; 142/2012, FJ 3; y 241/2012, FJ 4; así como las Sentencias del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, caso *Malone c. Reino Unido*, § 84 y, de 3 de abril de 2007, caso *Copland c. Reino Unido*, § 43).

De ahí que siendo dos diversos derechos fundamentales los que pueden verse afectados en el acceso a la información contenida en dispositivos de almacenamiento masivo, aunque el texto legal –art. 588 sexies c) 4- no contenga una neta diferenciación, la autorización judicial deberá fijar, tal y como exige el art. 588 sexies c), los términos y el alcance del registro, exigiendo una motivación “ad hoc” específica, relativa a la intromisión, no sólo en el ámbito de la intimidad, sino también en el ámbito protegido por el derecho fundamental al secreto de las comunicaciones, que justifique la extensión en el caso concreto del examen de las llamadas o datos relativos a comunicaciones que puedan guardarse en el dispositivo de almacenamiento masivo.

Sería deseable que el texto legal introdujese esta diferenciación, de la misma forma que lo ha hecho en relación con la incautación del dispositivo en un registro domiciliario, o la incautación del mismo fuera del domicilio, que no legitiman por sí mismas el acceso al contenido de los mismos, debiendo el Juez Instructor, en consecuencia, resolver expresamente, si el acceso al terminal debe extenderse también a los datos relativos a las comunicaciones electrónicas.

Así se deduce también los términos claramente delimitados por la doctrina constitucional ya mencionada, entre otras, por la STC 115/2013, de modo que la policía judicial podría llevar a cabo el examen directo de los datos contenidos en dispositivo incautado, salvo cuando se refieran a los datos relativos a las comunicaciones electrónicas, en cuyo caso únicamente cabe acceder con

autorización judicial, sin que los supuestos de urgencia constituyan excepción alguna (art. 18.3 CE).

En suma, el diferente régimen jurídico en cuanto a salvaguardas y protección del derecho de intimidad y el derecho secreto de las comunicaciones, requiere una valoración específica en la motivación del auto autorizante a la hora de determinar los términos y el alcance del registro.

¿Cabe trasladar a la lectura de los correos electrónicos las mismas garantías respecto a la apertura de correspondencia privada?

Nuestra LECRim recoge diversas cautelas respecto a la apertura de la correspondencia privada. Por ejemplo, el art. 584 establece que para la apertura y registro de la correspondencia postal será citado el interesado. Éste o la persona que designe podrá presenciar la operación. El art. 586 añade que la operación se practicará abriendo el Juez por sí mismo la correspondencia, y después de leerla para sí, apartará la que haga referencia a los hechos de la causa y cuya conservación considere necesaria. Los sobres y hojas de esta correspondencia, después de haber tomado el mismo Juez las notas necesarias para la práctica de otras diligencias de investigación a que la correspondencia diere motivo, se rubricarán por el Secretario judicial y se sellarán con el sello del Juzgado, encerrándolo todo después en otro sobre, al que se pondrá el rótulo necesario, conservándose durante el sumario, también bajo responsabilidad del Secretario judicial. Este pliego podrá abrirse cuantas veces el Juez lo considere preciso, citando previamente al interesado.

Este tipo de cautelas, basadas en la exigencia de proporcionalidad y en la menor lesividad en el derecho a la intimidad, no están previstas para la lectura de correos electrónicos, sin que parezca que, en términos de injerencia, exista mayor justificación para la adopción de dichas cautelas respecto al correo postal y no respecto al correo electrónico.

Sería deseable, desde luego, en atención a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, que así se hiciera, restringiendo la injerencia a lo realmente relevante para la causa, y restringiendo también el círculo de personas que accedan al conocimiento de ámbitos privados.

No obstante, la dificultad práctica ha sido puesta de manifiesto entre los participantes del seminario, ante la ingente cantidad de correos electrónicos que hoy en día puede albergar la bandeja de entrada de un investigado.

En cualquier caso, debería huirse de búsquedas prospectivas que permitan indagar en la totalidad del correo electrónico, sino únicamente respecto de aquellos correos en los que concurra causa probable.

No obstante, proceder en la forma antedicha se considera, cuando menos, una buena práctica en la apertura de los correos electrónicos, citando al investigado ante el Juez para llevar a cabo tal diligencia de apertura.

¿Cómo se lleva a cabo el volcado de estos datos? ¿Debe estar presente el Letrado de la Administración de Justicia? ¿Y el letrado de la defensa? ¿Qué medidas deben adoptarse para garantizar la autenticidad e integridad de los datos conservados?

Sobre esta cuestión hay un vacío legal. El 588 sexies c) dice que el auto que permita la medida de acceso a los datos contenidos en un dispositivo de almacenamiento masivo de información (ordenador, terminales de telefonía móvil, Smartphone, dispositivos de almacenamiento como USB…) y autorice la realización de copias de los datos informáticos, fijará las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial. No especifica nada sobre cómo debe hacerse el volcado y qué medidas puede adoptar el/a juez/a para preservar la integridad de los datos.

Presencia del Letrado de la Administración de Justicia. La mayoría de asistentes al seminario consideraba que no era necesaria su presencia ya que se trabaja con copias clónicas y que con los requisitos de firma electrónica o digital o hash, se garantiza que no se puede modificar su contenido y por tanto que no ha sido alterado. Se sigue por tanto la doctrina del Tribunal Supremo, seguida por ejemplo en su sentencia 342/2013, que revisa el caso de condena por 50 delitos de descubrimiento y revelación de secretos, un delito de distribución de pornografía infantil…. Se intervienen varios ordenadores y la defensa alega que el volcado de información se realizó sin que interviniera el LAJ, sin la presencia del interesado ni de su defensa y sin que conste la herramienta utilizada por las fuerzas y cuerpos de seguridad para proceder a ese volcado. Los ordenadores fueron incautados en la entrada y registro efectuada bajo la fe del LAJ que extendió el acta correspondiente. El material intervenido quedó en el Juzgado y en presencia del LAJ y previa autorización judicial los agentes procedieron al desprecinto de los discos duros de los tres ordenadores y al volcado de su contenido. Una vez terminada la diligencia, el material intervenido quedó nuevamente precintado y en poder de los agentes de policía intervinientes. Y aunque en el volcado estuvo presente el LAJ, sí dice el Tribunal Supremo que conviene *recordar que la jurisprudencia de esta Sala no ha considerado que la práctica de las operaciones técnicas de volcado exija como presupuesto de validez la intervención del Secretario judicial. La STS 15 noviembre 1999, aborda una alegación referida a la nulidad de la diligencia practicada por ausencia del Secretario*

en los siguientes términos: "... en lo que se refiere a lo que se denomina «volcaje de datos», su práctica se llevó a cabo con todas las garantías exigidas por la ley. En primer lugar, la entrada y registro se realizó de forma correcta y con la intervención del secretario judicial que cumplió estrictamente con las previsiones procesales y ocupó los tres ordenadores, los disquetes y el ordenador personal. Lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia. En esta sentencia, el Tribunal Supremo reitera lo ya dicho en su sentencia 256/2008 en la que el análisis de la información de los ordenadores intervenidos –que ya estaban a disposición del Juzgado- se llevó a cabo en la sede policial y sin presencia del LAJ. Pero el Tribunal Supremo considera que *esa presencia que se reclama habría sido, de facto, tan inútil -y, por tanto, innecesaria- como la que pudiera darse en el desarrollo de cualquier otra de las muchas imaginables en cuya técnica el fedatario judicial no fuera experto. Por eso, no habría nada que objetar a la intervención de los ordenadores y tampoco al modo en que fueron examinados".* En definitiva, según la doctrina del Tribunal Supremo, la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica. Lo decisivo es que, ya sea mediante la intervención de aquél durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado.

Presencia del letrado de la defensa. Hay un Auto de interés del Tribunal Supremo, nº 425/2016, dictado con ocasión de inadmitir el recurso de casación contra la sentencia. Se refiere al supuesto en el que se practica una entrada y registro en el que el auto autorizaba la aprehensión de los efectos e instrumentos procedentes de las conductas delictivas investigadas (falsedad de tarjetas de crédito y estafas). Entre ellos se encontró un pen-drive y se solicitó por la policía judicial autorización para el volcado, acordándose judicialmente que éste se realizara mediante la fe pública del Secretario Judicial y que una vez realizado se entregara la copia a los agentes y que la pericia se efectuara sobre esa copia. Se practicó el volcado extendiéndose la diligencia por el LAJ que hizo constar que el contenido del pen-drive se trasladaba a un pen-drive virgen, sin ninguna irregularidad en la cadena de custodia. La defensa recurrió alegando que no fue citado, ni él ni su letrado para el acto del volcado, asimilándolo a la apertura de la correspondencia privada. El Tribunal Supremo considera que *dicha actividad no consiste en seleccionar archivos concretos, sino realizar una copia. Y por tanto la presencia del imputado en la diligencia de volcado, en cuanto que no se toma ni aparta nada, sino que consiste meramente en la realización de la copia, no se justifica en dotar de mayor garantía a la operación de volcado, pues la misma cuenta con la presencia del Secretario Judicial, que da fe del traspaso de datos desde el soporte aprehendido a otro virgen.* Aunque ya hemos visto

que tampoco considera necesaria la presencia del LAJ en el volcado. Para el Tribunal Supremo no sería presupuesto de validez del acto, desplazando la cuestión al ámbito de la valoración de la prueba, ya que todos los aspectos del volcado que se quieran cuestionar por las defensas tales como por ejemplo la metodología técnica empleada por los agentes policiales, se pueden contradecir en el plenario mediante el interrogatorio de los agentes de policía que verificó el dictamen pericial o incluso la defensa puede aportar otro dictamen pericial.

Como hemos dicho, la mayoría de asistentes al seminario consideraba que no era necesaria la presencia del LAJ. Sin embargo, hay otra opinión que sí considera precisa dicha asistencia en el volcado y en la realización de las copias del contenido del dispositivo, ya que para poder hacer copias hay que acceder al contenido del dispositivo y se puede alterar, por lo que la presencia del LAJ es necesaria para asegurar la integridad de los datos y del contenido volcado. De hecho, a diferencia de lo que ocurre con las intervenciones telefónicas, en las que el artículo 588 ter f) especifica las medidas técnicas que garantizar la autenticidad e integridad de las copias de las grabaciones del SITEL: *sistema de sellado o firma electrónica avanzado… desde el ordenador central a los soportes digitales.* A diferencia, decimos, no hay precepto similar o garantías precisas similares en el registro de dispositivos de almacenamiento masivo de información, ya que el artículo 588 sexies c) encomienda al/a juez/a que fie las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación. El Anteproyecto de 2011 se refería en su artículo 347 a "herramientas informáticas" reiterando la idea de que para poder impugnar la autenticidad o integridad de los datos, era necesario que la impugnación se basara en indicios objetivos de manipulación, y en ese caso el tribunal haría una comprobación pericial.

¿Habría que observar algún tipo de garantía especial en el caso de que los archivos se encuentren en la nube alojados en otro país?

El art. 588 sépties a) prevé la posibilidad de que, con ocasión de un registro remoto sobre equipos informáticos, cuando los agentes comprueben que los datos buscados están almacenados en otro sistema informático o partes del mismo, puedan solicitar una ampliación de la autorización judicial.

Ahora bien, la cuestión resulta más problemática cuando los datos buscados se encuentran alojados en la nube o en un sistema alojado en otro país, lo que hace precisa la entrada en juego de las normas de cooperación internacional.

No es suficiente, pues, en estos caso, con que los agentes técnicamente puedan tener acceso a esos otros sistemas informáticos o partes del mismo, esto es, que los agentes técnicamente puedan acceder a la nube a través del ordenador registrado. Al encontrarse los datos en un servidor alojado en un país diferente,

bajo su jurisdicción, necesariamente han de entrar en juego las normas sobre cooperación internacional, estos es, la posibilidad de solicitar una orden de preservación de datos, sin perjuicio de aquellos otros supuestos en los que los agentes quedarían facultados, en virtud del art. 32 de la Convención sobre la Ciberdelincuencia (Budapest, 2001), que regulan el acceso transfronterizo a los datos de forma unilateral, entre las Partes signatarias, como excepción al principio de territorialidad, pero bajo circunstancias limitadas, dado que al encontrarse esos datos alojados en jurisdicciones extranjeras o en la nube, el concepto de soberanía nacional persiste.

Así el artículo 32 del Convenio sobre ciberdelincuencia establece como requisitos que se produzca con libre y voluntario consentimiento legítimamente emitido por el titular de los datos, o en segundo lugar, que se trate de fuentes abiertas al público. En ambos casos se podrá acceder, sin tomar en cuenta dónde se encuentra localizado geográficamente el dato.

La Guidance Note nº 3 emitida por Cybercrime Convention Committee (T-CY) de fecha 3 de diciembre de 2014, en relación con el artículo 32 del Convenio, cita algunos ejemplos (p.e. cuando los agentes acceden al e-mail de una persona que puede estar almacenado en los servidores alojados en otro país, y la persona puede recuperar este correo a través de su bandeja de correo electrónico, y voluntariamente permite el acceso a los agentes; o cuando un delincuente es arrestado y su correo electrónico está abierto, y consiente que la policía acceda a la cuenta –con el cumplimiento de los requisitos que para la emisión de este consentimiento requiera cada país-, aunque los policías estén seguros de que los datos de ese correo están localizados en otro país.

En ambos casos, la policía podrá acceder al dato bajo la cobertura que proporciona el artículo 32 del Convenio, pues en otro caso, al encontrarse dichos archivos bajo la jurisdicción de otro Estado, debería acudirse a los mecanismos de cooperación judicial mutua. En estos casos, añade la Nota, no se requiere una notificación al país donde se encuentran alojados los datos, aunque tampoco se excluye.

Esta medida, según indica la citada nota, resulta aplicable entre las partes que han suscrito este convenio, pero no cubre los supuestos de datos alojados en otro país que no sea parte del Convenio, o cuando se desconozca el lugar donde los datos se encuentran almacenados.

Quizá un nuevo Protocolo al citado Convenio, o los esfuerzos que en esta materia se están llevando a cabo en el seno de la Comisión Europea, logren ampliar el ámbito de las investigaciones en la nube, dado que dichas previsiones convencionales, que se remontan al año 2001, han quedado claramente desfasadas.

¿Pueden los padres acceder a los teléfonos móviles de sus hijos?

Para responder a esta pregunta nos remitimos a la STS 864/2015 sobre el child grooming o ciberacoso a menores. El caso se descubre porque la madre de una de las menores, sospechando que su hija menor de edad pudiera ser víctima de un delito a través de las redes sociales, accede a su cuenta abierta en Facebook sin contar con el consentimiento de la hija. La defensa recurre al considerar nula la prueba de los mensajes de whatssapp y de facebook cruzados entre el acusado con las menores al haber accedido la madre a su contenido sin contar con la autorización de su hija, habiéndose vulnerado, a entender del recurrente, los derechos a la intimidad y al secreto de las comunicaciones. Considera que no concurría la nota de proporcionalidad ya que la menor estaba en comisaría y las conversaciones no se podían destruir, con lo que ningún perjuicio se causaba en esperar la autorización judicial.

La primera premisa de partida es que una persona menor de 15 años tiene que otorgar el consentimiento a sus padres o tutor para que accedan y puedan desvelar los mensajes que en la cuenta de su perfil de facebook tiene, siempre y cuando el menor o la menor tengan las suficientes condiciones de madurez. Remite al artículo 4.1 de la Ley de Protección del Menor 1/1996 que dispone que *los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones".* Y en su artículo 4.5 establece que *los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros".* Asimismo, se completa con la Ley 1/1982, de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad y a la Propia Imagen, que establece que *el consentimiento deberá prestarse por ellos mismos (menores) si sus condiciones de madurez lo permiten.*

La segunda premisa de la que parte la sentencia analizada es de la distinción entre la afectación a un derecho fundamental –inviolabilidad del domicilio o secreto de las comunicaciones- que requieren autorización judicial, del derecho a la intimidad o privacidad que no lo requiere, y que de hecho puede acceder en determinados supuestos de urgencia la policía judicial.

La tercera premisa de la que parte es de la función tuitiva de la madre o del titular de la patria potestad respecto de la menor. *No puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente en que las evidencias apuntaban inequívocamente en esa dirección* –ser su hija víctima de un delito- *. Se trataba además de actividad delictiva no agotada, sino viva: es objetivo prioritario hacerla cesar.*

¿Puede el empresario acceder a los equipos informáticos de la empresa asignados a un empleado? ¿Tiene el trabajador en este contexto expectativa de confidencialidad?

Resulta inevitable la referencia a la reciente STEDH Gran Sala de 5 de septiembre de 2017 (Barbulescu c. Rumanía), que anula la anterior, dictada el 12 de enero de 2016 por el propio Tribunal, que proporciona un elenco de reglas relativas a la intimidad y el secreto de las comunicaciones en el ámbito laboral, en línea con el voto particular que efectuó el Juez Pinto en la STEDH de 12/01/2016 revocada:

"Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace/ Los trabajadores no abandonan cada mañana sus derechos a la intimidad y a la protección de datos cada mañana en la puerta de su trabajo"

Se debate en dicha sentencia el control del uso de internet (mensajería instantánea) por un trabajador en su puesto de trabajo y la utilización de los datos obtenidos para justificar su despido, concluyendo la existencia de violación del art. 8 CEDH. El empresario había controlado durante cierto tiempo las comunicaciones de una cuenta de "Yahoo Messenger" que el trabajador había sido invitado a abrir para responder a las solicitudes de información de los clientes, y los registros obtenidos durante los procedimientos internos de control mostraban que el trabajador había intercambiado mensajes de naturaleza estrictamente privada con terceros, existiendo un reglamento interior que prohibía la utilización de los ordenadores de la empresa para fines personales.

Considera el TEDH que el trabajador había sido informado de la prohibición de uso de internet para fines personales impuesta por el reglamento interno de la empresa, pero no fue informado con carácter previo del alcance y de la naturaleza del control de sus comunicaciones por el empresario, ni tampoco de la posibilidad de que éste accediese al contenido mismo de sus comunicaciones.

Tomando en cuenta de que la vulneración del derecho a la vida privada y de su derecho al secreto de las comunicaciones la produjo un empresario privado, el TEDH considera necesario plantearse el siguiente test:

- ¿El trabajador ha sido informado de la posibilidad de que el empresario adopte medidas de vigilancia de su correspondencia y de sus otras comunicaciones, así como de la puesta en práctica de tales medidas?

- ¿Cuál ha sido el alcance de la vigilancia realizada por el empresario y el grado de intrusión en la vida privada del empleado?

- ¿El empresario ha proporcionado motivos que justifiquen la vigilancia de las comunicaciones del trabajador?

- ¿Hubiera sido posible emplear un sistema de vigilancia conforme a medios y medidas menos intrusivas que el acceso directo al contenido de las comunicaciones del empleado?

- ¿Cuáles han sido las consecuencias de la vigilancia para el trabajador que ha sido objeto de las mismas?

- ¿El trabajador ha recibido las debidas garantías, en particular cuando las medidas de vigilancia del empresario tenían un carácter intrusivo?

En el caso concreto considera el TEDH que el trabajador no consta hubiera sido informado con carácter previo del alcance y la naturaleza de la vigilancia llevada a cabo por el empresario, ni de la posibilidad de que éste tuviera acceso al contenido mismo de sus comunicaciones, es decir, no había sido advertido previamente de la posibilidad de que su empresario empelase medidas de vigilancia, así como del alcance y naturaleza de las mismas. Tampoco verifica el TEDH la presencia de razones legítimas que justifiquen la puesta en marcha de la vigilancia de las comunicaciones del trabajador, ni si el objetivo perseguido por el empresario hubiera podido ser alcanzado por métodos menos intrusivos que el acceso al contenido mismo de las comunicaciones del trabajador.

Esta doctrina quizá imponga una revisión de nuestra doctrina constitucional representada, fundamentalmente, por las STC 241/12 y STC 170/13, pues la mera prohibición por convenio colectivo o por reglamento interior del uso del ordenador para fines personales no supone por sí misma una supresión de la "expectativa de intimidad" del trabajador, exigiendo los siguientes estándares mínimos en los casos de vigilancia de las comunicaciones por correo electrónico, en particular cuando la cuenta de correo y el ordenador sean de propiedad de la empresa:

- Información previa al trabajador *de la posibilidad de que el empresario adopte medidas de vigilancia de su correspondencia y de sus otras comunicaciones, así como de la puesta en práctica de tales medidas. El carácter previo supone que la información ha de ser anterior al inicio de la vigilancia.*

- Ha de valorarse el alcance de la vigilancia realizada por el empresario y el grado de intrusión en la vida privada del empleado. Tal valoración exigirá poner en relación la finalidad concreta pretendida por el empresario y los medios utilizados para ello. Por ejemplo, para saber si el trabajador usa el teléfono de la empresa para llamadas privadas es absolutamente innecesario el acceso al contenido de las llamadas, basta con conocer los titulares de los números marcados.

- El empresario ha de proporcionar motivos que justifiquen la vigilancia de las comunicaciones del trabajador, más allá del art. 20.3 ET. El TEDH se refiere claramente a motivos concretos.

- La vigilancia ha de ser proporcionada: hay que determinar si hubiera sido posible emplear un sistema de vigilancia conforme a medios y medidas menos intrusivas que el acceso directo al contenido de las comunicaciones del empleado.

- Hay que tener en cuenta y considerar cuáles han sido las consecuencias de la vigilancia para el trabajador que ha sido objeto de las mismas. Téngase en

cuenta que el trabajador ha hecho uso de un Derecho fundamental y que el despido es la máxima sanción.

- El trabajador debe haber recibido las debidas garantías, en particular cuando las medidas de vigilancia del empresario tenían un carácter intrusivo.

La sentencia referida afecta nuestra doctrina constitucional al respecto, sentencias 241/2012 y 170/2013, que deberá ser revisada bajo los parámetros establecidos por el TEDH. En ellas se minimiza el derecho al secreto de las comunicaciones del trabajador, ya que consideran que la prohibición por la empresa o por convenio colectivo de utilizar el correo electrónico o las herramientas informáticas para usos distintos del laboral, permite al empresario controlar la utilización de dichas herramientas por el empleado, lo que implica controlar sus comunicaciones y sus contenidos, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

¿Qué derechos pueden verse afectados en un registro remoto? ¿qué tipo de software puede ser utilizado? ¿qué tipo de límites o salvaguardas cabe establecer?

La primera parte ya está contestada en cuestiones anteriores.

El software que debe utilizarse ha de ser el menos invasivo de modo que solamente permita el acceso a los datos relevantes para la causa. Así lo exige el artículo 588 septies a) cuando establece que la resolución judicial que adopte la medida deberá concretar su alcance, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información. Lo habitual será que la policía judicial solicitante ya especifique en la petición el software posible a utilizar ya que el/a juez/a normalmente no tendrá conocimientos tan especializados para su elección. No obstante, sí corresponde al juez/a garantizar que el software utilizado sea el menos invasivo y se limite solamente a captar los datos relevantes para evitar intromisiones innecesarias en el ámbito de privacidad de la persona interesada.

¿Qué tipo de archivos podría intercambiar un agente encubierto online?

La figura del llamado agente encubierto “online” se regula de forma novedosa en el art. 282 bis 6 LECRIM en los siguientes términos:

6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, con autorización específica para ello, podrá 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.*

Con este apartado, se pretende otorgar al agente encubierto mayor margen de actuación acorde a la exención prevista en el apartado 5 del mismo precepto, como característica definidora que separa una actuación policial ordinaria (en la que puede haber ocultación) y una operación con agente encubierto.

No obstante, el precepto plantea diversa problemática, pues, en primer lugar, el apartado 5 exige para tal exención que guarde la debida proporcionalidad y no constituya una provocación al delito. Precisamente, el intercambio de archivos ilícitos que no posea el sujeto investigado podría considerarse como delito provocado.

Por otro lado, plantea un dilema moral y victimológico difícil de superar, por ejemplo, cuando se trate de archivos de pornografía infantil, lo que provocaría una -aún mayor- lesión en bienes jurídicos constitucionalmente protegidos, pues en el momento en el que el sujeto comparta este archivo, la policía deja de tener un control efectivo sobre el mismo y el efecto lesivo podría multiplicarse exponencialmente llegando a muchas más personas no controladas por los agentes.

¿Son susceptibles de manipulación las evidencias electrónicas?

Evidentemente, p*or* su especial naturaleza, las herramientas TIC hacen posible la simulación total o parcial de contenidos, resultando, en ocasiones, sumamente fácil, con los conocimientos adecuados, hacerse con el control de la cuenta de otro usuario, suplantar la identidad de terceras personas, modificar contenidos, etc. Múltiples páginas web muestran, paso a paso, lo fácil que puede resultar manipular tales evidencias electrónicas. La fácil manipulación de las evidencias digitales (tanto en cuanto a su existencia, como al origen, destino o contenido, hacen que la modificación de datos, su distorsión o manipulación, pueda producirse de forma relativamente fácil y frecuente, lo que necesariamente implica que los tribunales deban valorar esta prueba “con cautelas”.

La STS nº 300/2015, de 19 de mayo, con motivo de la impugnación de falta de autenticidad de los diálogos mantenidos a través de Tuenti, pone de relieve que la posibilidad de una manipulación de los archivos digitales, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la

prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso, según indica la STS nº 300/15, la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

No obstante, en ese caso concreto, no se estimó precisa tal prueba pericial, pues concurrían dos razones, a juicio del TS, que excluían cualquier duda. La primera, el hecho de que la propia víctima pusiera a disposición del Juez de instrucción su contraseña de Tuenti con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial. La segunda, el hecho de que el interlocutor con el que se relacionaba la víctima fue propuesto como testigo y acudió al plenario.

Vemos, pues, como el problema de la valoración de la prueba electrónica no difiere en demasía de los principios generales de valoración de la prueba, debiendo tomar en consideración la posición de las partes frente a dichas evidencias y su eventual régimen de impugnación, para valorar el elemento probatorio en soporte electrónico de forma conjunta e interrelacionada con el resto de elementos probatorios aportados al proceso.

El Dictamen nº 1/2016 de la FGE sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas, indica que:

Tanto en el caso de que se impugnen las capturas de pantalla aportadas al procedimiento, como el propio archivo electrónico en el que se recoge el contenido cuestionado, podrá ser necesario practicar –según el extremo que se impugne- diligencias de prueba para acreditar la existencia de la comunicación, su origen, destino o contenido, pero no en todos los casos resultará imprescindible la realización de prueba pericial. Dicha diligencia sólo puede resultar inexcusable cuando no exista posibilidad de acreditar aquéllos extremos por otros medios, tales como la declaración de otros destinatarios de la comunicación, la aportación por el administrador de una red social, previa autorización judicial, del contenido cuestionado u otros. Incluso, cuando lo que se discuta sea la identificación del emisor de una comunicación, quizá sea suficiente la aportación de los datos de tráfico relativos a un determinado proceso comunicativo. Todo ello sin olvidar la posibilidad de que haya sido utilizada alguna forma mensajería electrónica certificada, circunstancia que solventará muchas de las dificultades planteadas.

En dicho dictamen, cuya lectura recomendamos, se analiza diversa problemática que se plantea en atención al sistema o mecanismo de comunicación o traslado de información utilizado, y, en consecuencia, a partir del cual puede generar el medio de prueba que se pretende aportar al proceso: a) mensajería instantánea; b) mensajes SMS o MMS; c) correo electrónico y d) comunicación a través de plataformas de redes sociales; así como las posibles vías en cada

supuesto para corroborar la autenticidad o integridad de los mensajes o contenidos cuya transmisión se pretende acreditar en el proceso mediante la reproducción en documento físico de dichos contenidos o la presentación del dispositivo de comunicación mismo.

E) DEBATE SOBRE INCORPORACIÓN AL PROCESO DE DATOS DE USUARIOS, TRÁFICO, Y CONTENIDO. AUXILIO JUDICIAL INTERNACIONAL.

¿Cabe acceder a los datos de comunicaciones electrónicas conservados por los proveedores de servicios? ¿En qué casos?

Resulta obligado traer a colación las SSTJUE de de 8 de abril de 2014 (asunto Digital Rights) y de 21 de diciembre de 2016 (asunto Tele2 Sverige).

La primera de ellas declaró la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la Directiva 2002/58/CE. Estimó el TJUE que la obligación de conservación de tales datos con carácter general y preventivo vulneraba el artículos 7 (vida privada y secreto de las comunicaciones) de la Carta de Derechos Fundamentales de la Unión Europea (vida privada y secreto de las comunicaciones), así como también vulneraba también el art. 8 (protección de datos personales) y el art. 52, apartado 1 (limitación de derechos prevista en la ley, necesaria, proporcional), del citado texto legal.

La posterior STJUE 21 de diciembre de 2016 ha clarificado y delimitado el alcance de la anterior STJUE, cuya lectura recomendamos.

Del juego de ambos pronunciamientos, en el futuro únicamente resultarán conformes al Derecho de la Unión Europea esquemas limitados de conservación preventiva de datos de comunicaciones electrónicas, basados en criterios particulares de carácter temporal, geográfico, o subjetivo, que además deberán respetar un elenco de garantías y salvaguardas que detalla el TJUE (***criterios objetivos delimitadores: subjetivos, temporales, o geográficos; normas claras y precisas; nivel adecuado de protección; conservación en territorio de la Unión; destrucción al término del periodo de conservación; control por autoridad independiente; acceso de los datos así conservados únicamente en casos de delincuencia grave o terrorismo, previa autorización judicial y con información a las personas afectadas***).

Como consecuencia de tales pronunciamientos del TJUE en muchos países europeos se ha declarado la inconstitucionalidad de las respectivas leyes

nacionales de desarrollo o han sido anuladas. Sin embargo, en nuestro país, hasta el momento no se han extraído, a nuestro juicio, las consecuencias interpretativas que, en virtud de lo dispuesto en el art. 4.1 LOPJ, a las que obliga la recepción de dichos pronunciamientos dictados por el TJUE.

En concreto, el precepto que debe centrar nuestra atención es el art. 588 ter j) LECRIM, que establece:

> ***Artículo 588 ter j. Datos obrantes en archivos automatizados de los prestadores de servicios.***
>
> *1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.*
>
> *2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.*

Según apunta el precepto, la conservación de datos por parte de los prestadores de servicios podría venir basada, por un lado, en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas, y por otro, por la propia iniciativa de los prestadores de servicios, bien por motivos comerciales o de otra índole. Debemos, por tanto, analizar, tras los pronunciamientos del TJUE, cuál es el ámbito de la conservación de datos admisible.

En cuanto al primer inciso, esto es, en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas, en nuestro país tal texto legal es la Ley 25/2007 que implementó la Directiva 2006/24/CE, que ha sido anulada por el TJUE. Nuestra ley 25/2007 sobre retención de datos relativos a las comunicaciones electrónicas, que establece un esquema de conservación preventiva y generalizada de datos, adolece de los mismos defectos que el TJUE apunta en la STS 21/12/2016 en relación con la legislación sueca, por lo que en virtud del principio de primacía del Derecho de la Unión deviene materialmente inaplicable, aunque, por el momento, no haya sido formalmente derogada, a diferencia de lo que ya ha sucedido en otros muchos países del UE.

Por tanto, a nuestro juicio, no cabrá invocar en el futuro la Ley 25/2007 como fundamento legal para obtener la cesión de datos conservados, pues tal conservación resulta contraria a los art. 7, 8 y 52.1 de la Carta, sino que habrá que acudir al art. 588 ter j) en los términos que a continuación expondremos.

Avanzando en nuestro análisis, el segundo inciso “por propia iniciativa por motivos comerciales o de otra índole” también debe ser interpretado a la luz de lo dispuesto en el art. 6 de la Directiva 2002/58, dado que la posibilidad de conservación de los datos de tráfico por parte de los proveedores de servicios queda restringida al plazo para impugnar la factura. Así lo establece el art. 6 de dicha Directiva, al indicar que los datos de tráfico deberán eliminarse o hacerse anónimos cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, y que únicamente podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones, autorizando este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. La determinación de este plazo puede suscitar cierta incertidumbre, que en el futuro deberá ser abordada y clarificada.

Es decir, la conservación de datos de tráfico únicamente está autorizada respecto de aquellos que sean necesarios a efectos de facturación, y más allá del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago este plazo máximo, dichos datos deben ser eliminados o hacerse anónimos, como expresamente exige el art. 6 de la Directiva.

De ahí que no existe margen legal, a tenor del art. 6 de la Directiva 2002/58 para que los proveedores de servicios conserven datos más allá del periodo de facturación, debiendo anonimizarlos o eliminarlos, a pesar de la dicción del art. 588 ter j) que parece dar a entender la posibilidad por parte de los proveedores de servicio de conservar los datos que apetezcan, lo que únicamente será posible tras la debida anonimización. Ello conllevaría la falta de validez como prueba en el proceso penal de aquellos datos que, por los motivos que sean, puedan permanecer en posesión de los prestadores de servicios, vulnerando la confidencialidad de los mismos y las salvaguardas que establece la Directiva, dado que la destrucción al término del periodo de conservación constituye una de sus exigencias fundamentales.

En tercer lugar, el art. 588 ter j) se está refiriendo a los datos que “*se encuentren vinculados a procesos de comunicación”, con lo que quedan excluidos* los datos de localización distintos de los datos de tráfico, a los que se refiere el art. 9 de la Directiva 2002/58, dado que estos datos de geolocalización distintos de los datos de tráfico, generados como consecuencia de la conectividad de los terminales con las estaciones BTS por la simple puesta a disposición del usuario del servicio de comunicaciones, no aparecen vinculados a un proceso de comunicación. A mayor abundamiento, el art. 9 de la Directiva 2002/58 establece que los datos de localización distintos de los datos de tráfico, solo podrán ser tratados si se hacen anónimos o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesario para la prestación de un servicio con valor añadido, por lo que

su conservación, tratamiento o acceso de dichos datos más allá de dicha previsión supondría un tratamiento también prohibido por la Directiva 2002/58.

Consecuencia de ello, es que la autorización judicial como presupuesto de acceso a los datos conservados, debe delimitar la posibilidad de acceso a aquellos datos cuya conservación sea conforme con el derecho de la Unión, esto es, aquellos datos que los prestadores de servicios conserven de forma legítima, dentro de los límites establecidos en la propia Directiva 2002/58 y la jurisprudencia del TJUE que los interpreta.

En definitiva, el art. 588 ter j) constituye ahora la base legal que actualmente posibilita la averiguación de datos conservados, aunque restringida su conservación y también la posibilidad de averiguación al periodo preciso para la facturación o aquel durante el cual pueda impugnarse legalmente la factura o exigirse el pago, en detrimento de la Ley 25/2007, que adolece de los mismos defectos que la legislación sueca a la que se refiere la STJUE de 21/12/2016.

Salvo que en el futuro el legislador desarrolle algún tipo de medida legislativa que permita la conservación concreta de datos -en función de criterios objetivos, territoriales, o subjetivos- adoptada de conformidad con lo dispuesto en el art. 15 de la misma Directiva, cumpliendo la hoja de ruta marcada por el TJUE y el catálogo de salvaguardas ya apuntadas.

¿Cabe cesión de datos de comunicaciones electrónicas en relación con un delito imprudente –pe, accidente aéreo, ferroviario, tráfico- u otros delitos de menor gravedad?

Surgen dudas en cuanto al ámbito delictivo respecto al cual, conforme al art. 588 ter j) LECRIM, cabe acordar el acceso a los datos conservados, que, en buena lógica, deben ser resueltas conforme a una interpretación gramatical y lógico sistemática.

En concreto, el Capítulo V "La interceptación de las comunicaciones telefónicas y telemáticas", del Título VIII ("*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*"), se compone de tres Secciones: la 1ª dedicada a las "*Disposiciones generales"*, que en realidad van referidas principalmente a la "intervención" (concepto más restringido que la "interceptación") de las comunicaciones telefónicas y telemáticas; la Sección 2.ª "*Incorporación al proceso de datos electrónicos de tráfico o asociados"*, integrada por un único precepto, el art. 588 ter j), cuyo análisis nos ocupa; y la Sección 3ª, se titula *"Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad".*

El art. 588 ter a), que encabeza la Sección 1ª, establece como presupuesto para la "interceptación" de las comunicaciones telefónicas y telemáticas que la investigación tenga por objeto alguno de los ***delitos a que se refiere el artículo 579.1*** de esta ley o ***delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación***.

Sin embargo, el art. 588 ter j), regulado en Sección distinta, no contiene ninguna remisión expresa ni limitación del ámbito objetivo, por lo que se plantea la duda de si -dado que constituye una forma de "interceptación" aunque no sea intervención propiamente en las comunicaciones telefónicas y telemáticas- resulta o no de aplicación el ámbito objetivo previsto en el art. 588 ter a).

La ubicación sistemática de ambos preceptos, en secciones distintas, pudiera dar a entender que el art. 588 ter a) únicamente resulta aplicable a la Sección 1ª, dedicada a la "intervención" de las comunicaciones, y no respecto a la 2ª, que regula específicamente la incorporación al proceso de datos conservados.

Pero como ya hemos referido, la Sección 2ª comprende un único precepto, el art. 588 ter j, y se encuentra incluida en el Capítulo V que se *titula "la interceptación de las comunicaciones telefónicas y telemáticas"*, que cubre un mayor espectro que la mera intervención de las comunicaciones que se regula en la Sección 1ª. Dado que el art. 588 ter a) se refiere a la "interceptación" de las comunicaciones telefónicas y telemáticas, y que el acceso a los datos conservados constituye una forma de "interceptación" de las comunicaciones, aunque no suponga su "intervención" propiamente dicha, debemos entender que el presupuesto de aplicación recogido en el art. 588 bis a) resulta también aplicable en relación con al acceso a los datos conservados.

Si se sigue esta línea interpretativa, probablemente debería también extrapolarse, por las mismas razones lógico sistemáticas, a la Sección 3ª del mismo Capítulo V, por ejemplo, a la averiguación de la titularidad de un número de teléfono o de cualquier otro medio de comunicación por parte del Ministerio Fiscal o la Policía Judicial, que se regula en el art. 588 ter m), esto es, restringiéndola al ámbito delictivo previsto en el art. 588 bis a), lo que parece que ofrezca una solución acertada.

Se pueden plantear numerosos supuestos delictivos, que no se encuentren incluidos en el ámbito del art. 579.1 LECRIM, o que tampoco hayan sido cometidos a través de instrumentos informáticos o servicios de comunicación, en los que el acceso a los datos conservados pueda proporcionar una prueba precisa para el esclarecimiento de los hechos investigados. Por ejemplo, la investigación de un grave accidente de tráfico, ferroviario, aéreo, etc. Resulta ciertamente dudoso, en base a lo expuesto, dado que no se ha cometido a través de medios telemáticos ni

tienen carácter doloso, que en este tipo de casos pueda accederse a los datos conservados.

Ello enlaza con una cuestión nuclear, esto es, el umbral de gravedad del delito investigado que debe identificarse para ordenar las diversas medidas de injerencia en el ámbito de las intervenciones de las comunicaciones y de la averiguación de datos de tráfico y de usuarios, que no tiene por qué tratarse de un umbral de gravedad coincidente en todas ellas.

Una interesante cuestión prejudicial planteada por la Sección 4ª de la AP de Tarragona (ponente Sr. Hernández) de fecha 6 de abril de 2016, en tramitación bajo el asunto C-207/16, tiene por objeto precisamente este dilema, dirigiéndose al TJUE para que aclare, en concreto, si la suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puede identificarse *únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos. Y en su caso, si se ajusta a los principios constitucionales de la Unión, utilizados por el TJUE en su sentencia de ocho de abril de 2014 como estándares de control estricto de la Directiva, la determinación de la gravedad del delito atendiendo solo a la pena imponible, cuál debería ser ese umbral mínimo, y si resultaría compatible con una previsión general de límite en tres años de prisión*.

En el caso concreto en el que se planteó dicha cuestión prejudicial, el Ministerio Fiscal interpuso recurso de apelación frente a la denegación por parte del Juez Instructor del acceso a los datos conservados en relación con un delito de robo con violencia, por no cubrir la exigencia prevista en el art. 1 de la Ley 25/2007, entendiendo por delito grave aquel que castiga con pena superior a 5 años, de conformidad con el art. 13 y 33 CP.

Ciertamente la STJUE de 21/12/2016 ha aportado diversos argumentos respecto a la gravedad de los delitos investigados, estableciendo que dicho acceso debe guardar la debida proporcionalidad con la gravedad que la injerencia que supone, y, por ello, adopta un criterio restringido, entendiendo que únicamente la **delincuencia grave** puede justificar dicho acceso, remitiéndose en este aspecto, por analogía, al concepto de delito grave empleado por el TEDH (STEDH de 4 de diciembre de 2015, Zakharov c. Rusia).

No obstante, creemos que cabe realizar una distinción relevante en este punto, según se restrinja el acceso al periodo de facturación de la empresa, esto es, al periodo normal de conservación de datos con fines comerciales, como límite temporal marcado por la Directiva 2002/58; o en función de un periodo de conservación mayor que se establezca legalmente en virtud de lo dispuesto en el

art. 15 de la Directiva, en los límites marcados en las citadas SSTJUE de 8/04/2014 y 21/12/2016.

Ello resulta especialmente trascendental en la persecución del cibercrimen, y para cumplir además con las exigencias que se derivan de la STEDH de 2 de diciembre de 2008 (Caso K.U. c. Finlandia), y las disposiciones contenidas en el Convenio sobre Cibercrimen, que a continuación abordamos:

- En el asunto K.U. c. Finlandia, el TEDH se enfrentó a un caso en el que se publicó un anuncio relativo a una persona joven de 12 años de edad que pretendidamente buscaba una relación íntima con un chico de su edad, requiriendo el padre del menor a la policía y a los tribunales finlandeses que identificasen a la persona que había publicado el falso anuncio. El proveedor de servicio rehusó proporcionar la identidad del titular de la dirección IP amparándose en la confidencialidad de las comunicaciones, y que la legislación finlandesa únicamente permitía la obtención de dichos datos en relación a determinados delitos, entre los que no se encontraba la calumnia o difamación, lo que asimismo confirmó el Tribunal de Apelación y el Tribunal Supremo. El TEDH, por el contrario, consideró que el art. 8 CEDH impone al Estado obligaciones positivas para un efectivo respeto a la vida privada o familiar (STEDH Airey v. Irlanda, 9 de octubre de 1979) y que estas obligaciones pueden exigir la adopción de medidas, incluso en el ámbito de las relaciones entre individuos, sobre todo en aquellos casos que se trate de actos graves que precisen un castigo penal (STEDH X and Y c. Holanda, §§ 23-24 y 27; August c. Reino Unido (dec.), no. 36505/02, 21/01/2003; y M.C. c. Bulgaria, no. 39272/98, § 150). En el caso concreto, expone el TEDH, la mera existencia del delito de calumnia o difamación alcanza muy limitados efectos disuasorios en ausencia de la posibilidad legal de identificar al responsable, entendiendo el TEDH que la obligación positiva del Estado de salvaguardar la integridad física y moral del menor debía extenderse a cuestiones relativas a la efectividad de una investigación criminal y de la disponibilidad de medios que permitan identificar al agresor, lo que no se pudo llevar a cabo en el caso concreto aduciendo la confidencialidad de los datos. En este aspecto, manifiesta el TEDH que aunque la libertad de expresión y la confidencialidad las comunicaciones son valores esenciales, y que los usuarios de las telecomunicaciones y de Internet deben tener la garantía de que su propia privacidad y libertad de expresión va a ser respetada, dicha garantía no puede ser absoluta, sino que debe ceder en ocasiones ante otros imperativos también legítimos como la prevención y descubrimiento del crimen, o la protección de los derechos fundamentales de otros, correspondiendo al legislador proporcionar el marco legal adecuado para la investigación de tales hechos, apreciando, por todo ello, violación del artículo 8 CEDH, al no disponer Finlandia, en ese momento, de medidas

legales efectivas que permitieran la averiguación del titular de la IP desde la que se efectúo ese anuncio.

En el caso analizado por el TEDH se trataba de un delito de calumnia o difamación cometido a través de internet que, en atención al rango penológico, podría ser considerado también en nuestro país como un delito de menor gravedad, respecto al cual el TEDH impuso, no obstante, la obligación positiva de implementar medidas legales efectivas que permitieran la investigación penal, sin la cual el efecto disuasorio derivado de la tipificación de los hechos como delito se debilitaría.

Hoy en día, las relaciones humanas se desarrollan cada vez más en modo virtual, y este último ámbito resulta propicio para la comisión de múltiples delitos, cuya penalidad puede no ser grave, pero cuya investigación pasa ineludiblemente por la averiguación de los datos conservados.

La limitación del acceso de los datos conservados a los delitos más graves generaría, sin duda, la práctica impunidad de gran parte de los delitos cometidos a través de internet o cuya prueba se encuentre en formato electrónico. Dicha impunidad no resulta asumible en un escenario actual y de futuro crecimiento exponencial de los llamados ciberdelitos.

- Junto a ello el Convenio sobre Cibercrimen, del Consejo de Europa (STE 185), ratificado por España, impone a los Estados parte la existencia de mecanismos legales que faciliten la investigación del cibercrimen y en general de los delitos cometidos por medio de sistemas informáticos o cuya prueba pueda obtenerse en formato electrónico. En la sección 2ª del capítulo II, regula diversas cuestiones procesales cuyo alcance va más allá de los delitos informáticos, dado que se aplicarán a cualquier delito cometido por medio de un sistema informático o cuando la evidencia se encuentre en formato electrónico, determinando las garantías aplicables, y asegurando las siguientes facultades procesales: *conservación inmediata de datos informáticos almacenados, preservación y divulgación inmediata de datos de tráfico, registro y confiscación de datos informáticos almacenados, recogida en tiempo real de datos informáticos, e interceptación de datos de contenido, así como diversas disposiciones en materia de competencia territorial y conflictos de jurisdicción*. No se recoge, entre las medidas previstas en el Convenio, la conservación generalizada y preventiva de datos.

De ahí que, a modo de recapitulación, la gravedad a la que se refiere el TJUE en su sentencia de 21/12/2016, según postulamos, deba ir necesariamente conectada a la gravedad de la injerencia que supone la conservación preventiva –aunque ahora necesariamente limitada por mor de la STJUE de 21/12/2016- de los datos relativos a las comunicaciones electrónicas. Ese carácter preventivo en la

conservación, por la grave injerencia que supone, debe ir asociado a mayores exigencias a la hora de autorizar el acceso a dichos datos conservados.

Sin embargo, en aquellos otros supuestos en los que no se produce tal conservación preventiva, debería garantizarse el acceso a los datos conservados por los proveedores de servicios, simplemente durante el periodo de facturación, también en relación con delitos de menor gravedad (por ejemplo, la calumnia o difamación a que se refirió la STEDH K.U. c. Finlandia), lo que encuentra fundamento en la diferente gravedad de la injerencia en uno u otro caso.

¿Qué datos conservados pueden facilitar los proveedores de servicios a los agentes policiales sin necesidad de autorización judicial? ¿Qué diferencias existen entre los artículos 588 ter j) –datos vinculados a procesos de comunicación- y 588 ter m) –datos de titularidad de teléfonos o medios de comunicación-?

El artículo 588 terj) exige autorización judicial para obtener la cesión de aquellos datos relativos a comunicaciones electrónicas conservados por los prestadores de servicios o personas que faciliten la comunicación, vinculados a procesos de comunicación.

En la medida en la que dichos datos quedan registrados en el mismo momento en el que la comunicación se está llevando a cabo, aunque sean tomados en consideración con posterioridad, resulta exigible la autorización judicial (STC 123/2002), como reiteradamente ha venido estableciendo nuestro TC, al proclamar que queda afectado el derecho al secreto de las comunicaciones tanto por la entrega de los listados de llamadas telefónicas por las compañías telefónicas como por el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil (por todas, SSTC 123/2002, FJ 6; 56/2003, FJ 3; 230/2007, FJ 2; 142/2012, FJ 3; y 241/2012, FJ 4; así como las Sentencias del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, caso *Malone c. Reino Unido*, § 84 y, de 3 de abril de 2007, caso *Copland c. Reino Unido*, § 43). Al tratarse de datos externos al proceso comunicativo que quedan registrados en el mismo momento en el que comunicación se está desarrollando, quedan englobados en el derecho al secreto de las comunicaciones, que requiere autorización judicial (art. 18.3 CE) para su averiguación.

A diferencia de este tipo de datos vinculados a procesos de comunicación, el artículo 588 ter m) recoge la posibilidad de que el Ministerio Fiscal o la Policía Judicial averigüen la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o en sentido inverso, precisen el número de teléfono o los datos identificativo de cualquier medio de comunicación, dirigiéndose directamente a los prestadores de servicios, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en un delito de desobediencia.

Los datos a los que se refiere este artículo únicamente hacen referencia a los datos de suscriptor, es decir, aquellos datos de mera titularidad o identificación. Cuestión diferente, como ya hemos abordado en otra de las cuestiones, es que la búsqueda de titularidades (p.e. IMEI) deba realizarse de forma entrecruzada asociada al IMSI, esto es, a través de procesos de comunicación, en cuyo caso las compañías vienen denegando la asistencia directamente solicitada por la Policía Judicial, requiriendo autorización judicial.

Precisamente la STS admite que *para delimitar los supuestos de exigencia de autorización judicial* debe de tomarse en cuenta la locución *"... que se encuentren vinculados a procesos de comunicación", utilizada por el art. 588 ter j) para delimitar los supuestos de exigencia de autorización judicial, indicando que a esta categoría pertenecerían aquellos datos que son generados e interferidos durante el desarrollo de una comunicación bidireccional."*

¿Qué problemática plantean los rastreos de direcciones de IP con ocasión de intercambios de archivos P2P en funciones de prevención de delitos? ¿Qué diferencias existen entre el art. 588 ter k –identificación y localización de direcciones IP por parte de la Policía Judicial- y el art. 588 ter m –averiguación de titularidades de un número de teléfono o medio de comunicación por la Policía Judicial?

El artículo 588 ter k establece la posibilidad, por parte de la Policía Judicial, de identificar direcciones IP, lo que es conocido como ciberpatrulleo, siempre que ésta se produzca en canales abiertos, indicando a continuación la necesidad de solicitar autorización judicial para obtener la identificación y localización del equipo o del dispositivo de conectividad o los datos de identificación personal del usuario.

Lo que contrasta con la posibilidad recogida en el art. 588 ter m) en la que se faculta directamente a la Policía Judicial o al Ministerio Fiscal, sin precisar autorización judicial, para averiguar la titularidad de un número de teléfono o de cualquier otro medio de comunicación.

Esta diferenciación encuentra explicación en el método de obtención de la IP, en el primer caso, tras establecer, en un canal abierto, una comunicación que posibilita la averiguación de la IP del sospechoso. Mientras que en el segundo caso, los métodos de obtención no vienen datos precisamente por su interceptación del proceso comunicativo, o ésta goza ya de autorización judicial.

En el primer caso, el Tribunal Supremo ya había afirmado que para acceder a tales códigos o datos no era necesaria autorización judicial al tratarse de datos públicos de Internet. Podemos citar en este sentido las STS 236/2008 y 1299/2011. En ellas se reconoce el carácter de dato personal de la dirección de IP y que, por tanto, no es indiferente para el proceso penal el sistema utilizado para la obtención de dicho dato. Sin embargo, afirma que no hay lesión al secreto de las comunicaciones y no se

precisa por tanto autorización judicial porque el dato es público, ya que por ejemplo utilizar un programa P2P para acceder a las IP que habían accedido a los hash que contenían pornografía infantil, *a esa información puede acceder cualquier usuario de la red, ya que la huella de la entrada, el IP, queda registrado siempre y eso lo sabe el usuario, y por tanto asume y consiente que muchos datos que incorpora a la red sean de conocimiento público para cualquier usuario de Internet. Asimismo, las claves identificativas, IP, no concretan a la persona usuario, sino sólo al ordenador que se ha usado. Es decir, los rastreos sólo afectan a datos públicos de Internet.*

¿Puede la policía judicial captar mediante artificios técnicos el IMSI o el IMEI sin autorización judicial? ¿Cabe identificar déficit de salvaguardas en el art. 588 ter l?

El art. 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Roma, 4.XI.1950) proclama el derecho al respeto a la vida privada y familiar, en los siguientes términos:

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El TEDH reitera la necesidad de previsión legal de las medidas injerentes, pero especialmente se refiere en sus análisis a la "calidad" que debe tener la Ley que regula este tipo de medidas. Recuerda el TEDH que en el contexto de medidas de vigilancia secreta, la Ley debe utilizar términos bastante claros para indicar en qué circunstancias y bajo qué condiciones faculta al Poder público para recurrir a tales medidas (ver, entre otros, Malone c. Reino Unido, del 2 de agosto de 1984, Valenzuela Contreras c. España, de 30 de julio de 1998, y Bykov c. Rusia). Teniendo en cuenta el riesgo de abusos inherente a cualquier sistema de vigilancia secreta, dichas medidas deben basarse en una Ley muy precisa, sobre todo considerando que la tecnología disponible es cada vez más sofisticada (SSTEDH Weber y Saravia c. Alemania; Asociación para la Integración Europea y los Derechos Humanos y Ekimdjiev, de 28 de junio de 2007; Liberty y otros c. Reino Unido, de 1 de julio de 2008; Iordachi y otros c. Moldavia, de 10 de febrero de 2009).

Este enfoque interpretativo constituye un sólido pilar con el que el TEDH se muestra muy estricto, destacando que en el ámbito de las medidas secretas de vigilancia, el propio Tribunal Europeo de Derechos Humanos debe quedar completamente satisfecho de que existen adecuadas y efectivas garantías contra el

abuso, aplicando un test de garantías, que exige que la Ley contenga los **tipos de delitos** que pueden dar lugar a una orden de interceptación; las **personas** a las que la medida puede ser aplicada; los **límites temporales** de la medida; el **procedimiento** para la obtención, uso y almacenamiento de los datos obtenidos; las **cautelas exigibles** en la transmisión de los datos a otras partes; y las **circunstancias** por las que los datos obtenidos deban ser borrados o destruidos.

El TEDH ha recalcado que debe quedar convencido de la existencia de garantías adecuadas y suficientes frente a los abusos, y esta apreciación dependerá del conjunto de las circunstancias de la causa, por ejemplo, el alcance y la duración de las medidas eventuales, los requisitos exigidos para ordenarlas (tipo de delitos, procedimiento, cautelas, etc), las autoridades competentes para permitirlas, ejecutarlas y controlarlas, el tipo de recurso proporcionado por el derecho interno, entre otras (Asociación para la Integración Europea y los Derechos Humanos y Ekimdjiev, con remisión a Klass. y otros c. Alemania , del 6 de septiembre de 1978).

Este programa de garantías, entendemos, no se cumple en el caso de los artificios técnicos empleados para averiguar de forma subrepticia el IMSI o el IMEI de un sospechoso, bien como paso previo a acordar una intervención telefónica, o bien como paso previo para la identificación real de un sospechoso o de las personas que con él se encuentran.

El art. 588 ter i) establece:

> *1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.*
>
> *2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.*
>
> *El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.*

El precepto no vincula necesariamente la averiguación del IMSI o IMEI con una posterior intervención de las comunicaciones, ya que en el primer párrafo se refiere a la necesidad de obtener un determinado número de abonado que resulte

indispensable para la investigación, y en el segundo apartado se refiere en términos facultativos, los agentes “podrán” solicitar la intervención de las comunicaciones.

En el caso de que no lleguen a solicitarla es evidente que se habrá desarrollado una actividad investigativa subrepticia carente de cualquier tipo de control en cuanto al tipo de delito, las **personas** a las que la medida puede ser aplicada, el procedimiento para la obtención, uso y almacenamiento de los datos obtenidos, las cautelas exigibles, o las circunstancias por las que los datos obtenidos deban ser borrados o destruidos. Es decir, si la intervención telefónica no llegase a ser solicitada, nadie tendría por qué enterarse de que se ha llevado a cabo dicha investigación subrepticia, empleando medios tecnológicos, para averiguar datos personales, protegidos por el derecho a la intimidad.

Este tipo de actuaciones queda, a nuestro juicio, al margen de las salvaguardas exigidas por el art. 8 CEDH. Incluso aunque posteriormente se solicite al Juez instructor la intervención telefónica a la que podrían estar preordenadas, la vulneración ya se habría consumado de antemano, quedando contaminados sus resultados.

Es curioso que el TS haya considerado nula la observación policial, sin orden judicial, de un domicilio realizada a distancia, mediante unos prismáticos y a través de una ventana, según doctrina sentada por la STS nº 329/2016, de 20 de abril, y sin embargo, valide el empleo de los llamados “IMSI CATCHERS” (SSTS nº 1115/2011, de 17 de noviembre,79/2011, de 15 de febrero;249/2008, de 20 de mayo;776/2008, de 18 de noviembre), destacando en tales pronunciamientos que la intervención judicial se produce “a posteriori” al tener que dirigirse la Policía a las operadoras en virtud de la Ley 25/2007, de 18 de octubre, de Conservación de Datos de las Comunicaciones Electrónicas, que incluye en el art. 3.1 los datos IMSI e IMEI para cuya cesión resulta exigible la preceptiva autorización judicial. En estos casos habrá de solicitarse mandamiento judicial. Reconoce la STS nº 249/2008, de 20 de mayo, que la información incorporada a la numeración IMSI es, sin duda alguna, un dato, en los términos de la legislación llamada a proteger la intimidad de los ciudadanos frente a la utilización de la informática (art. 18.4 de la CE), considerando el TS que el acceso de ese dato en el marco de una investigación criminal -nunca con carácter puramente exploratorio-, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional.

Ahora bien, con la nueva regulación legal en la mano, obtenido el IMSI o IMEI del sujeto o sujetos sospechosos, la Policía podrá acudir a las operadoras para solicitar la identidad de los usuarios, al amparo del art. 588 ter m), con lo cual, la garantía de judicialidad a la que se referían las SSTS antes citadas brilla por su ausencia en todo el proceso.

No debemos olvidar que una de las funcionalidades del IMSI CATCHER permite a la Policía, por ejemplo, averiguar la identidad de un grupo de personas que se hayan reunido en determinado lugar, y que todo ello puede desarrollarse fuera del control judicial.

Si la averiguación del IMSI o IMEI está preordenada a una intervención telefónica, debería recabarse autorización judicial ya desde ese inicio de la investigación, validando el Juzgador desde un inicio el empleo de medios tecnológicos subrepticios como el IMSI cátcher, y si se dirige a averiguar la identidad de personas reunidas, debería igualmente recabarse autorización judicial, de la misma forma que el uso de prismáticos la requiere, según doctrina del TS, como término comparativo de fácil comprensión.

¿Cabe hablar de "intimidad compartida" en el ámbito de la pareja o familiar? ¿Qué problemática plantea la violencia de género cometida a través de medios tecnológicos (redes sociales, correo electrónico, SMS, etc)?

La STS 569/2013 (cuyo voto particular se tratará en la última cuestión ya que dio lugar o al menos recoge la actual doctrina sobre la obtención ilícita de fuentes de prueba por un particular) reconoce que la relación de pareja no cancela la intimidad y no supone para los integrantes de la misma la desaparición de todo espacio íntimo, de ese reducto personalísimo que es la proyección más auténtica de la individualidad misma. Únicamente conlleva una transferencia recíproca o recíproco acceso de cada uno a algunos aspectos de la intimidad del otro que antes le pertenecían en exclusiva. Pero sin que desaparezca su derecho a un espacio íntimo, a su intimidad. Por tanto, debemos partir de la idea de expectativa razonable de intimidad.

¿Cabe reconocer valor probatorio a la información obtenida ilícitamente por un particular?

Necesariamente partimos de la STS 116/2017, caso Falciani, que recoge una doctrina que ya venía utilizando y como hemos dicho en la cuestión anterior, fue objeto del voto particular en la STS 569/2013. Y se refiere a los efectos de la ilicitud en la obtención de la prueba atribuible, no a órganos del Estado, sino a particulares. En el voto particular referido, el caso analizado era el de una mujer que roba a su ex pareja unas grabaciones que guarda en el coche porque cree que le ha sido infiel, y lo que descubre es a su ex marido abusando de su cuñada cuando duerme. La STS mayoritaria absuelve al acusado por prueba ilícita pero en el voto particular ya se introducen una serie de matices y distinciones que se acogen posteriormente. Parte de la regla general de que la inutilizabilidad de la prueba obtenida con violación de derechos se predica de todos los casos y de todos los procesos, más allá de que el agente infractor sea estatal o sólo un particular. Pero, esta regla admite modulaciones en el caso de particulares. Primero, cuando se haya accedido a la misma como un

hallazgo casual y no de manera intencionada para conseguir material de cara a un proceso. Es decir, no se están buscando pruebas y por tanto la actuación escapa a las previsiones del art. 11.1 LOPJ. *Si quien atentó contra la intimidad actuaba guiado por el móvil de recabar elementos probatorios para mejorar o alcanzar una posición procesal, habrá que tachar de ilícita e inutilizable tal prueba. Cuando la vulneración del derecho fundamental no iba presidida por ese propósito nos movemos en un terreno muy diferente.* En estos casos no se busca disuadir de la tentación de investigar con medios o métodos ilegítimos ya que no se buscaba ese propósito.

En la STS 116/2017, caso Falciani, al condenado se le investigaba por estar incluido en la lista Falciani. Hervé Falciani era un informático que trabajaba en el banco HSBC en su sucursal en Suiza y realizó desde su puesto de trabajo un listado de unas 130.000 personas posibles evasores fiscales al tener cuentas no declaradas en dicha entidad bancaria. Cruzó los datos de los documentos bancarios a los que accedió, hizo el perfil de los contribuyentes que habían ocultado sus ganancias a Hacienda y confeccionó un listado. Fue detenido en Francia y la policía francesa, en un registro de su domicilio de Niza practicado en virtud de una solicitud de cooperación internacional suiza que le acusaba de un delito contra el secreto bancario, encontró los archivos informáticos con el listado. En España, la Agencia Tributaria pidió a Francia que le remitiese información y en concreto el listado de los contribuyentes sujetos a la jurisdicción fiscal española. Francia entregó un CD con varios archivos de personas y entidades con fondos, activos y valores en dicho banco suizo. Cada persona física o jurídica se identificaba con un código llamado BUP y contenía información con el nombre, fecha de nacimiento, profesión, dirección, país, teléfono, cuentas en el HSBC y patrimonio. La causa examinada por el Tribunal Supremo se inicia contra una persona física incluida en dicho listado. La agencia tributaria le inspeccionó, con todos esos datos a su disposición, y fue condenado por la Audiencia Nacional como autor de dos delitos contra la hacienda pública. El condenado recurrió alegando la nulidad de la prueba al haber sido obtenida de forma ilegítima y el Tribunal Supremo lo desestimó al considerar que la prueba fue obtenida por un particular que cuando la obtuvo no tuvo intención alguna de utilizarla en un proceso sino simplemente de lucrarse vendiendo los datos. La defensa alegó que las autoridades españolas no pueden receptar documentación o información obtenida ilícitamente, aunque el lugar de origen de la prueba ilícita sea un Estado extranjero. Así, señala primero que Falciani accedió a datos protegidos y reservados de manera ilícita vulnerando la intimidad de los clientes del banco, no existiendo resolución judicial autorizando dicho acceso. Pero es que además del acceso ilegítimo hubo luego un tratamiento posterior de esos datos. Así, la ficha BUP no era documentación oficial del banco ya que los archivos informáticos que se encontraron en el ordenador de Falciani por la policía en el registro domiciliario no eran los originales del banco, y por otra parte, las autoridades francesas no entregaron una copia íntegra de esos archivos del ordenador de Falciani a las autoridades españolas sino que trataron los datos, dado que extractaron la información del ordenador y la trataron informáticamente antes de remitirla a las autoridades españolas. Por lo que había habido una manipulación informática por las autoridades francesas. Señala que el Tribunal de Casación francés en sentencia de 31 de enero de 2012 ratificó la sentencia de la Corte de Apelación de París que consideró

en un caso también de la lista de Falciani que esos datos (documentos) eran robados y por tanto constituían prueba ilegítima. El Tribunal Supremo, resuelve basándose en el concepto de prueba ilícita, y distinguiendo entre el Estado o un particular. El artículo 11 LOPJ prohíbe valorar pruebas obtenidas con vulneración de derechos fundamentales pero para proteger frente a los excesos del Estado en la investigación del delito. Y la actuación de un particular nada tiene que ver con la de un agente al servicio del Estado, por lo que se puede valorar una fuente de prueba obtenida por un particular con absoluta desconexión de toda actividad estatal y ajena en su origen a la voluntad de prefabricar pruebas. No persigue sobreproteger al delincuente que se ve encausado con el respaldo de pruebas que le han sido arrebatadas por un particular que cuando actuaba no pensaba directamente en prefabricar elementos de cargo utilizables en un proceso penal ulterior. Es por tanto relevante la ausencia de toda finalidad de preconstitución probatoria por el particular que proporciona las pruebas, siendo determinante que nunca, de forma directa o indirecta, haya actuado el particular como una pieza camuflada del Estado al servicio de la investigación penal. En el caso analizado, Falciani quería obtener un rédito económico vendiendo el listado, pero nunca actuó como agente al servicio del Estado para castigar a evasores fiscales. No se trataba de *pruebas obtenidas* con el objetivo, directo o indirecto, de hacerlas valer en un proceso.