Sentencias de Pleno de la Sala Segunda del Tribunal Supremo durante el año 2025

EDUARDO DE URBANO CASTRILLO

Abogado Of Counsel. Doctor en Derecho

Ex Magistrado Coordinador del Gabinete Técnico
de la Sala Segunda del Tribunal Supremo

En el año 2025, la Sala Segunda del Tribunal Supremo ha dictado cuatro «sentencias de pleno», tres menos que en el año 2024, haciendo uso de la posibilidad recogida en el artículo 264 de la LOPJ de unificar criterios, que desde 2019 ha sustituido a los clásicos «acuerdos del Pleno», que no se expresaban en una sentencia sino en un criterio doctrinal sobre una cuestión controvertida que se redactada en un texto, se daba a conocer públicamente y al que luego le seguían las sentencias correspondientes que seguían o debían seguir el sentido interpretativo alcanzado en el Pleno de la Sala, reuniones en las que se buscaba la unanimidad.

De hecho, cuando no se alcanzaba ese consenso, y la Sala se dividía, se evitaba tomar acuerdos por mayoría, porque entonces quedaba en evidencia que no había un criterio sólido sobre el tema o cuestión examinada y era más que razonable no publicar un supuesto acuerdo de nuestro más Alto Tribunal, que en realidad no existía.

Pero en la actualidad, y desde hace unos años, las sentencias de Pleno se configuran como auténtica jurisprudencia, en el sentido del artículo 1.6 CC, reforzada porque vienen avaladas por un estudio y debate de todos los Magistrados de la Sala, que no sólo expresan una doctrina al respecto, sino que resuelven un caso determinado, con el efecto jurídico-procesal que ello supone.

Ciertamente, y como ya advertimos en la Crónica del pasado año, esta nueva fórmula no evita las discrepancias de criterio, pues todas menos una de las sentencias de pleno dictadas en 2024 por la Sala de lo Penal, contaron con votos particulares. Es decir, sólo se alcanzó la

unanimidad en una única sentencia, la STS núm. 265/2024, de 18 de marzo.

Dicho lo anterior, en el año 2025, las sentencias de Pleno dictadas por el máximo órgano de la jurisdicción penal, en las que, por cierto, no se produjeron votos particulares, fueron las siguientes:

STS núm. 487/2025, de 28 de mayo.
STS núm. 818/2025, de 8 de octubre.
STS núm. 849/2025, de 16 de octubre.
STS núm. 854/2025, de 16 de octubre.

1. STS núm. 487/2025, de 28 de mayo; Roj: STS 2606/2025 - ECLI: ES: TS:2025:2606

Cuestión: ¿Es necesaria la convivencia para aplicar los artículos 153.2, 171.7 y 173.4 del Código Penal?

Respuesta: No se entra a resolver la cuestión en atención a que se planteó como «cuestión nueva».

Sentencia decepcionante porque no hubiera sido necesario llevar a Pleno un caso en que con la aplicación de la conocida doctrina de la «cuestión nueva», hubiera bastado para inadmitir, o en su caso desestimar el recurso, sin necesidad de entrar en el fondo y por supuesto sin que hubiera que convocar al Pleno de la Sala para resolver esa cuestión.

En efecto, considera la Sala, como cuestión nueva, pues no fue alegada con anterioridad, si en los delitos entre parientes, referenciados en los artículos antes citados, es necesario para su aplicación que exista una convivencia previa entre agente y Víctima cuando el sujeto pasivo son ascendientes, descendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente.

El recurso de casación que dio lugar a la presente sentencia plenaria, se admitió «a trámite al considerar existía "interés casacional" a la vista de que se alegaba que existía sentencias» (1) que se apartaban del criterio sostenido por la Audiencia de Valencia que desestimó en apelación el recurso.

La cuestión que se suscitaba era que en el caso presente, la recurrente –la condenada– y su madre no convivían, por lo que se aducía que: ha de degradarse el delito de lesiones del artículo 153.2 CP a delito leve, aunque a tenor del principio acusatorio ha de ser absuelta;

(1) En concreto: Sentencia 587/05, de 23 de junio de 2006, de la Sección 10.ª de la Audiencia Provincial de Barcelona y la Sentencia 395/05 de 11 de julio de la Sección 1.ª de Audiencia Provincial de Madrid.

en cuanto al delito leve de amenazas del artículo 171.7 CP, ha de ser absuelta por no existir convivencia entre madre e hija, principio acusatorio y ser la amenaza leve y carente de dolo; y respecto al delito leve de injurias del artículo 173.4 CP, al no existir convivencia, y tratarse de injuria leve entre particulares que ha quedado destipificada, ha de ser absuelta.

Pero nos quedamos sin respuesta al caso, ya que –se dice– «la cuestión planteada en el recurso no fue articulada ni en la instancia ante el Juzgado de lo Penal ni en apelación ante la Audiencia dado que el único motivo planteado fue el error en la valoración de la prueba practicada en el acto del juicio oral».

Y, en consecuencia, el recurso casacional planteaba una «cuestión nueva», es decir, que se pudo plantear en apelación y sin embargo no se hizo, por lo que es de aplicación la jurisprudencia consolidada de la Sala (*vid*. SSTS 73/2022, de 27-1; 985/2022, de 21-12; 676/2024, de 27-6; 990/2024, de 7-11; 291/2025, de 27-3) que afirma que «el recurso de casación por infracción de ley se circunscribe a los errores legales que pudo haber cometido el juzgador al enjuiciar los temas sometidos a su consideración por las partes, o, en su caso, el Tribunal de apelación al conocer del correspondiente recurso. Lo que implica que no puedan formularse *ex novo y per saltum* alegaciones relativas a otros que, pudiendo haberlo sido, no fueron suscitados con anterioridad».

A continuación, la Sala sostiene que «lo decidido por un Juzgado de lo Penal no es susceptible de casación; solo de apelación. Es lo resuelto en apelación lo que puede acceder a casación. Y en la casación se ventila la conformidad a derecho de la sentencia de apelación que, si es correcta, solo podrá pronunciarse sobre lo impugnado, no sobre otras cuestiones que las partes no cuestionan en sus recursos. Es más, si resolviese sobre otros puntos no impugnados, aunque su solución fuese hipotéticamente acertada en el fondo, habría que anularla en casación ante la queja de cualquier parte por no haberse ajustado a ese dogma elemental y clásico: *tantum devolutum quantum apellatum* (*vid*. art. 465.5 LEC)».

Y se desarrolla esta conocida tesis, de forma amplia –y como se dijo– sin entrar en la interesante cuestión que planteaba el recurso, que quedó, por tanto, sin respuesta.

Se reitera pues, la doctrina que sobre la materia tiene establecida la Sala Segunda de nuestro Tribual Supremo, que sintetizamos del siguiente modo:

«Pueden aducirse en casación nuevos argumentos (*v. gr.* se pidió en apelación que se suprimiese la reincidencia por no tratarse de delito de la misma naturaleza y en casación se alega, además, que el antecedente

estaba cancelado); pero no podrán introducirse nuevas pretensiones impugnatorias (no se discutió la reincidencia en la apelación y en casación se lucha por suprimir la agravante: sobre esa cuestión no hay ningún pronunciamiento de la Audiencia; por tanto no se puede reprochar a la Audiencia una decisión inexistente. No se puede anular una sentencia de la Audiencia que ha resuelto de forma impecable todo lo que le presentó para resolver; y que, también haciendo lo que debía hacer, no se ha pronunciado sobre otras cuestiones). Las pretensiones impugnatorias no admiten el efecto Guadiana: desaparecen en la apelación y reaparecen sorpresivamente en una ulterior impugnación. En el momento en que se consiente una decisión no impugnándola queda expulsada esa cuestión de la controversia, ha dejado de formar parte del objeto procesal de la apelación y, por ende, de la casación. Las impugnaciones sucesivas han de ser un *continuum* guardando congruencia unas con otras.

En el ámbito penal así vino a afirmarlo la jurisprudencia desde que se introdujo un recurso de apelación previo a la casación en el procedimiento del jurado. Antes el problema del recurso *per saltum* no aparecía: no existía una segunda instancia previa a la casación (el diseño era o apelación o casación; pero no apelación más casación). Con la generalización de la segunda instancia han comenzado a reproducirse supuestos, cada vez más frecuentes, en que aparece esta disfunción».

Pero constituye doctrina común a todas las Salas de este Tribunal Supremo, civil, contencioso-administrativa y social, que coinciden en la idea de que la parte que suscita en el recurso de casación una cuestión que no planteó antes en el recurso previo, o en su caso, en la instancia, no puede ser atendida. La respuesta a esa pretensión novedosa ha de ser la inadmisión o, en su caso, la pura y simple desestimación sin analizar el fondo, en cuanto sobre este no hay pronunciamiento de la sentencia cuya corrección ha de examinarse (naturaleza revisora de la casación), no podía haberlo porque no era objeto de impugnación».

Por todo ello, se procede a la desestimación sin necesidad de abordar el problema de fondo planteado en virtud de la doctrina expuesta, a tenor de la cual esa es la respuesta en fase de decisión cuando se constata un óbice de admisibilidad.

La verdad es que la sentencia no supone ninguna novedad por lo que –como se dijo– no se entiende por qué se llevó el recurso al Pleno de la Sala, salvo –se nos ocurre decirlo, como hipótesis– por si la trascendencia del tema de fondo hubiera podido excepcionar tan arraigada doctrina, en virtud del derecho a la tutela judicial efectiva que consagra el artículo 24.1 de nuestra Carta Magna y que en más de una ocasión los Tribunales utilizan para entrar en el fondo de cuestiones, formal o procesalmente, mal planteadas.

2. STS núm. 818/2025, de 8 de octubre; Roj: STS 4393/2025 - ECLI: ES: TS:2025:4393

Cuestión: Posibilidad de reevaluar la decisión de absolver por delitos de coacciones y prevaricación administrativa; y revocabilidad en casación del pronunciamiento sobre las costas procesales imponibles a la acusación.

Respuesta: En el primer caso, no se dieron los elementos típicos de dichos delitos; y en cuanto a las costas, a pesar de la dificultad de introducir esta cuestión en casación, se dice que es posible su examen y únicamente si se aprecia una total falta de motivación o una decisión irracional al respecto, cabrá casar la sentencia en ese particular.

A) Empezando por la cuestión sustantiva, se plantea una reevaluación de la decisión de absolver por delitos de coacciones y prevaricación administrativa. Y se resuelve el recurso del siguiente modo:

1. Por lo que se refiere al delito de coacciones, la Audiencia Provincial tuvo dudas de la real comisión de los hechos. Consideró insuficiente la prueba practicada para acreditar que las posibles víctimas se hubieran visto determinadas a actuar en contra de su voluntad por la acción de los acusados.

Es una valoración no solo llena de lógica, sino la más lógica, se dice en la sentencia objeto del recurso.

Las Salas sentenciadoras han dado cumplimiento a su deber de motivación y, al tiempo, han dado satisfacción, paralelamente, al derecho a la tutela judicial efectiva que asiste a las partes. Los razonamientos, ni siquiera remotamente, pueden calificarse de arbitrarios; o huérfanos de lógica; o caprichosos. Antes al contrario, realizan una correcta ponderación de los elementos de cargo ofrecidos por la acusación para respaldar sus imputaciones y se da una fundada respuesta a la pretensión condenatoria formulada por el recurrente, aunque sea contraria a sus intereses.

Esta Sala de casación no puede volver a evaluar la verificación probatoria de los hechos que sostiene la parte recurrente. Concurren pruebas personales relevantes valoradas por el Tribunal que las presenció en términos que debemos respetar.

Dos líneas llevan a refrendar esta conclusión. En primer lugar, los límites impuestos a la revocación de las sentencias absolutorias, particularmente cuando son fruto de la valoración probatoria, conforme a la doctrina del Tribunal Europeo de Derechos Humanos, del Tribunal Constitucional y del Tribunal Supremo (*vid.* las SSTC citadas en el primer fundamento). La absolución se construye sobre la base de la

valoración de prueba personal, lo que corresponde, sin otro límite que el respeto a las reglas del raciocinio humano, al Tribunal de instancia, que la ha percibido directamente y en su totalidad.

2. En cuanto al delito de prevaricación administrativa, se trata de un delito que precisa de una declaración de voluntad de contenido decisorio que afecte a los administrados. El delito, además, exige que la resolución resulte arbitraria, en el sentido de contrariar la razón, la justicia y las leyes, desviándose de la «normopraxis» administrativa de una manera flagrante, notoria y patente, esto es, que el sujeto activo dicte una resolución que no sea el resultado de la aplicación del ordenamiento jurídico sino, pura y simplemente, de una voluntad injustificable revestida de una aparente fuente de normatividad.

Por «resolución» hay que entender aquellos actos administrativos de carácter constitutivo y declarativo, excluyéndose los actos carentes de carácter decisorio (por todas, STS 769/2022, de 15 de septiembre).

B) Abordando ya el tema de las costas, inicia la resolución del Tribunal Supremo, el examen de la cuestión planteada, indicando que más allá de la dudosa naturaleza sustantiva de la norma supuestamente infringida (art. 240.3 LECrim) –a diferencia del art. 123 CP–, es patente la dificultad de introducir en casación esa temática a través del artículo 849.1.º LECrim (*vid*. STS 297/2022, de 24 de marzo). Ni el artículo 240 LECrim es norma sustantiva; ni es tema en el que la fiscalización radique en comprobar la correcta subsunción de los hechos: *item* más, en el *factum* no encontraremos normalmente referencia alguna a las circunstancias determinantes de la condena en costas.

Sin embargo, la praxis de este Tribunal, empero, viene admitiendo la discusión en casación de ese tipo de pronunciamientos (no asimilables en rigor a los basados en el Código Penal: art. 123 CP). No deja de ser paradójico si nos asomamos a la clásica jurisprudencia civil tremendamente reticente a abrir el debate casacional a los temas de costas dada su naturaleza estrictamente procesal y no ser las cuestiones procesales propias de la casación (por todas SSTS Sala 1.ª 607/2018, de 23 de octubre o 174/2021, de 29 de marzo –ésta para abrir una excepción ATS Sala 1.ª de 26 de septiembre de 2018 –rec. 1470/2016–). Un replanteamiento de esta praxis enlazaría con la jurisprudencia más clásica (STS de 18 de enero de 1887) reanudando –valga la imagen– un tracto sucesivo interrumpido hace muchos años. Pero –se dice– lo hacemos ahora.

Dicha cuestión, el de la revisión en materia de costas en casación, canalizada en el caso a través del artículo 852 LECrim, esto es, por presunta infracción de precepto constitucional, es resuelta mediante

una clara respuesta: **«en esa vía bastará constatar que el pronunciamiento está racionalmente motivado –lo que no puede discutirse en este supuesto– para cerrar la discusión. Solo en casos de absoluta falta de motivación o irracionalidad de la decisión cabrá casar la sentencia en ese particular. En los restantes supuestos hemos de respetar la decisión del Tribunal de instancia ya revisada en apelación».**

Por eso, también se procede en este punto, a la desestimación del recurso, ya que en el caso examinado no se discute que hubo una respuesta motivada.

3. STS núm. 849/2025, de 16 de octubre; Roj: STS 4646/2025 - ECLI: ES: TS:2025:4646

Cuestión: Requisitos para aplicar el artículo 197.2 CP.

Respuesta: La mera utilización de una contraseña personal ajena para acceder a los datos incluidos en un ordenador, llena los requisitos del delito de revelación de secretos.

El caso se refiere a una persona que, sin tener la titulación de enfermero, ejerció como tal durante años y además se introdujo en el ordenador de una enfermera del centro, logrando acceder a todo su contenido, entrando, sin autorización, en diversas carpetas que contenían archivos privados y personales de la enfermera.

La condena por intrusismo no fue objeto de discusión. Sí, en cambio, el delito de revelación de secretos que el TSJ consideró inexistente, en base a este razonamiento:

«Frente a todo ello, y con los hechos probados y con los fundamentos de derecho de la sentencia no podemos comprobar que se ha invadido el ámbito personal reservado, o que la libertad informática de esta persona haya resultado afectada. En algún párrafo aislado de los fundamentos de derecho se recoge "real y ciertamente se produjo por el acusado una intromisión no autorizada en la intimidad de Soledad, accediendo a datos sensibles y reservados de su vida privada allí guardados", pero ni en los hechos probados se dice a qué "datos sensibles y reservados de su vida privada allí guardados" son a los que se ha accedido porque solo recoge las carpetas ya citadas, ni en los fundamentos de derecho explica cuáles son esos datos sensibles y reservados a los que ha accedido el acusado y cuándo se ha producido ese acceso porque el único que se recoge como probado es el del día 11 de octubre de 2018».

El Tribunal Supremo, en la sentencia casacional, discrepa ya que: «La sentencia impugnada hace una lectura incompleta del relato fáctico. Es cierto que los hechos probados refieren la existencia de determinadas carpetas y su nomenclatura, pero el tribunal de instancia hizo algunas otras precisiones fácticas que el tribunal de apelación ha omitido.

Así, cuando hace alusión al uso que la denunciante hacía de su ordenador afirma que lo utilizaba diariamente «para elaborar sus particulares e individuales modelos de "plantillas o planillas" de los usuarios de la residencia, como de ordenador personal propio con clave personal y no accesible a terceros sin su permiso, dado el contenido reservado y datos sensibles de su vida privada allí incorporados, así como su correo electrónico personal». También dice que el día en que el acusado accedió al ordenador, una vez que había obtenido fraudulentamente la clave de la denunciante, entró en determinadas carpetas y añade que se trataba de carpetas «perfectamente identificadas con archivos privados y personales».

Por lo tanto, el relato fáctico describe, por más que lo haga de forma sucinta y poco precisa, que el ordenador tenía información personal, lo que desautoriza el principal argumento de la sentencia impugnada para considerar atípicos los hechos».

Y a continuación se detalla la doctrina que se exige para aplicar el artículo 197.2 CP, y que sintetizamos, del siguiente modo:

Es cierto –se dice en la sentencia– que no basta para colmar las exigencias típicas del tipo previsto en el artículo 197.2 CP el simple acceso a un dispositivo que pueda almacenar información personal, como lo es un ordenador. Se hace necesario que se acceda a esa información y en este caso los hechos probados describen ese acceso, como, por otra parte, ocurre siempre, salvo supuestos excepcionales en que un ordenador no haya sido utilizado y esté complemente vacío de información, circunstancia que desde luego no concurre en este caso.

Precisado lo anterior, resulta obligado reseñar que el artículo 197.2 CP sanciona «al que, sin estar autorizado, acceda por cualquier medio a datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».

Luego, se cita –entre otras– la STS 634/2019, de 19 de diciembre, que afirma que, **en principio, todos los datos personales automatizados son sensibles** en cuanto la ley no establece distinciones en su

protección y ninguno de ellos es inocuo una vez informatizado porque pueden ser manipulados y fuente de información. No existen, por consiguiente, datos personales automatizados reservados y no reservados, por lo que debe interpretarse que todos los datos personales automatizados quedan protegidos penalmente.

Y saliendo al paso de un equívoco bastante generalizado, se dice: «**No importa la trascendencia e importancia objetiva de los datos personales y familiares.** No cabe, pues, diferenciar a efectos de protección entre datos o elementos «objetivamente» relevantes para la intimidad, que serían los únicos susceptibles de protección penal, y datos «inocuos» cuya escasa significación los situaría directamente fuera de la intimidad penalmente protegida. En esta dirección la STS 725/2004. de 11 de junio, nos dice que el artículo 197. 2 CP no hace distinciones respecto del objeto de la acción que tengan fundamento en normas no penales y se refiere a «datos reservados de carácter personal o familiar» registrados en soportes informáticos, electrónicos o telemáticos de archivos o registros públicos o privados. Es decir, que **el legislador ha querido alcanzar todos los datos de estas características porque, indudablemente, todos son merecedores de protección penal.**

En el caso a que se refiere la presente sentencia de pleno, y según se declara en el relato fáctico de la sentencia, el acusado se introdujo en el despacho de la enfermera afectada y «valiéndose de la contraseña que, previamente había obtenido en junio con la ayuda de un pendrive que introdujo en el equipo informático, logró acceder a todo su contenido».

Pues bien, **la obtención fraudulenta de la clave del ordenador ya es de por sí un acceso no consentido a un dato personal reservado de la denunciante. La clave, que es un identificador de su titular, permite el acceso a toda la información que pueda existir en el ordenador, y que, por lo mismo, constituye per se un dato personal reservado protegido por el artículo 197.2 del Código Penal.**

La clave de un ordenador personal es la llave, la puerta de acceso a todo el contenido de ese ordenador en el que ordinariamente se almacena información reservada del titular y de la misma forma que hemos dicho que la obtención indebida de «un identificador en línea constituye un dato personal susceptible de protección» porque permite identificar a su titular, también es protegible y sancionable penalmente la obtención de la clave del ordenador personal de otra persona en cuanto da acceso a toda la información personal almacenada en el dispositivo, sin que sea

preciso una descripción detallada de su contenido una vez que consta que el autor no se limitó a obtener la clave sino que accedió a sus distintas carpetas y contenido y ese acceso generalizado a toda la información del ordenador integra el perjuicio que exige el precepto aplicado.

En efecto, según la literalidad del artículo 197.2 CP el apoderamiento, utilización o modificación de datos personales de carácter personal requiere que se realice «en perjuicio del titular o de tercero» y hemos declarado, mediante una interpretación integradora, que ese perjuicio también es exigible en la conducta de simple acceso (SSTS 1328/2009, de 30 de diciembre y 40/2016, de 3 de febrero).

Y finalmente, para determinar la existencia del perjuicio, se diferencia entre que se trate de datos especialmente sensible o no.

En el primer supuesto, en caso de acceso a datos especialmente sensibles, que tienen una penalidad agravada (art. 197.5 CP) la propia relevancia de los datos determina la existencia del perjuicio.

Y se entiende por dato especialmente sensible, de acuerdo con el Reglamento de Protección de Datos (art. 9) y el artículo 195.5 citado los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física, así como los referidos a víctimas menores de edad o personas con discapacidad necesitadas de especial protección.

En otro caso, cuando los datos no sean especialmente sensibles habrá de acreditarse la existencia de un perjuicio.

Por eso, aunque en los hechos no consta que los datos personales a los que se accedió fueran especialmente sensibles, **el acceso indiscriminado a todo el contenido de un ordenador personal, que puede y ordinariamente incluye información personal muy amplia y variada, integra el perjuicio típico que exige el artículo 197.2 CP.**

Por tanto, los hechos probados son subsumibles en el artículo 197.2 CP lo que determina la estimación del recurso y de ese modo se restaura la inicial doble condena que estableció la Audiencia Provincial, con imposición de la misma pena que ésta estableció.

Esta es la única sentencia de las cuatro «de pleno» dictadas en 2025, en la que el Tribunal Supremo estimó el recurso de casación, y en este caso, de modo parcial.

4. STS núm. 854/2025, de 16 de octubre; Roj: STS 4526/2025-ECLI: ES: TS:2025:4526

Cuestión: Tratamiento procesal de *Encrochat.*

Respuesta: Es válido siempre que no vulnere los derechos o garantías observables en el proceso concreto de que se trate.

Confirma la Sala de lo Penal la sentencia de la Audiencia Nacional, dictada por su Sala de Apelación, en un caso de narcotráfico en el que se examina *Encrochat*, una red de comunicaciones encriptada que utilizan principalmente organizaciones criminales y que constituye la primera sentencia del Tribunal Supremo sobre este sistema de mensajería.

La sentencia avala las pruebas utilizadas para la sentencia condenatoria y lo hace tras examinar en qué consiste *Encrochat* y su correcta aplicación al caso, habida cuenta que se impugnó el valor probatorio de las conversaciones que las autoridades judiciales francesas obtuvieron de la mencionada plataforma *Encrochat*, llegadas a España a través de la OEI que formuló la Fiscalía Antidroga, y posteriormente incorporadas al procedimiento.

Las quejas de los recurrentes se centraron en la vulneración del derecho al secreto de las comunicaciones por proceder el material incautado de una actuación prospectiva, no autorizada judicialmente en España, cuestionando además el proceso de asignación de identidades a los usuarios de la plataforma.

La sentencia, de cierta amplitud, trata el tema en tres partes que va examinando sucesivamente: primero, describe el marco general sobre *Encrochat*, a continuación, analiza jurisprudencia y doctrina del TEDH, y acaba con la aplicación al caso, en el que en el acto del juicio se ratificaron los informes elaborados por la Policía Judicial, con el preceptivo sometimiento de sus autores al interrogatorio contradictorio.

1. MARCO GENERAL SOBRE *ENCROCHAT*

Comienza el análisis del tema, con el escrito de impugnación presentado por el Ministerio Fiscal, en el que se dan unas pinceladas sobre dicho tipo de sistema de comunicación encriptada.

Indica la sentencia que el MF señala que «Aunque se dispone de información sobre el actual uso por organizaciones criminales de más de 50 nuevas plataformas de mensajes encriptados, en este momento *EncroChat, SKY-ECC, ANOM y EXCLU* son las que, ya intervenidas,

son origen de las comunicaciones que están siendo utilizadas como prueba en los distintos procedimientos».

Se trata en todos los casos –sigue el Escrito del Ministerio Público– de «aplicaciones informáticas que se instalan en los teléfonos (algunos, como *EncroChat,* preferentemente en un determinado tipo de terminales) y permiten una comunicación privada de mensajes escritos, fotos, vídeos, audios, que busca evitar la interceptación por las autoridades judiciales. Instalada la *app* para encriptar las comunicaciones se cierran el resto de las funciones del teléfono móvil.

Cada una tiene características técnicas distintas de las que derivaran seguramente algunas particularidades también en su tratamiento procesal. Como característica común los terminales carecen de identificación del usuario de la SIM, resultando que en *EncroChat* la identificación del usuario se hacía por apodos y en SKYECC a través de un código alfanumérico».

La importancia de la «interceptación de los mensajes de estas plataformas es muy grande ya que están proporcionando a los investigadores europeos un panorama actual del tráfico de drogas y la delincuencia organizada, dado que "gran parte de los procedimientos judiciales en trámite sobre narcotráfico trasnacional grave están basados, total o parcialmente, en prueba obtenida a través de las intervenciones de las plataformas de encriptados"». Y es que «alrededor del 90 % de las comunicaciones interceptadas se refieren al tráfico de drogas, principalmente de cocaína; el resto tienen que ver con algunos casos de asesinatos o secuestros relacionados en general con el narcotráfico».

Y también se da un dato que no es baladí: «No se ha detectado que los usuarios de estos sistemas hayan hecho uso de ellos para tratar sobre asuntos de carácter legal».

Los precios del sistema encriptado son altos, en *EncroChat* se habla de unos 1.000 euros el terminal y unos 1.500 trimestrales. Los canales de distribución de la aplicación eran restringidos, a través de circuitos privados en internet en la mayoría de los casos. La seguridad y privacidad se concibe máxima y en *EncroChat* se permitía la autodestrucción de mensajes, borrado de contraseñas y borrado de pánico que fue utilizado cuando se dieron cuenta de la intervención de *EncroChat.* En el momento de la explotación de *EncroChat* los usuarios que recibieron un mensaje con la alerta de la intervención se pasó a SKY pero, en todo caso, no se impidió el acceso a los datos ya que las conversaciones estaban ya intervenidas».

A continuación, la sentencia comienza con una breve introducción sobre el sistema *Encrochat,* sus características generales y su examen respecto al caso de origen. Lo resumimos con toda la brevedad posible.

1. *Características generales*

Sobre las particulares características, funcionamiento y vicisitudes de *EncroChat,* con carácter introductorio, se recurre en primer lugar a la STJUE (Gran Sala) de 30 de abril de 2024, asunto M. N. (C-670/22) –apartados 19 y 20–:

– En el marco de una investigación llevada a cabo por las autoridades francesas, se puso de manifiesto que algunos investigados utilizaban teléfonos móviles encriptados, que funcionaban bajo una licencia denominada *EncroChat*, para cometer delitos relacionados principalmente con el tráfico de estupefacientes.

– Esos teléfonos móviles permitían, gracias a un software especial y a un material modificado, establecer, a través de un servidor instalado en Roubaix (Francia), una comunicación cifrada de extremo a extremo, que no podía ser intervenida mediante métodos tradicionales de investigación.

– Con mayor detalle, la Sentencia del Tribunal Supremo Federal Alemán de 2 de marzo de 2022 - *BGH 5 StR 457/21 - Beschluss vom 2. März 2022 (LG Hamburg)*- indica que los teléfonos se anunciaban con las siguientes características: i) anonimato garantizado (sin conexión del dispositivo, ni de la tarjeta SIM a la cuenta del cliente); ii) plataforma Android personalizada (interfaz totalmente cifrada desde el principio, centrada en la seguridad y la confidencialidad, con configuraciones de usuario simplificadas); iii) sistema operativo dual (los usuarios pueden usar el sistema operativo Android estándar o *EncroChat*, ya que ambos sistemas operativos se incluyen con cada dispositivo); iv) tecnología de vanguardia (terminales telefónicos especialmente diseñados y configurados para aumentar la seguridad mediante el bloqueo de la cámara, el micrófono, el GPS y el puerto USB); v) borrado automático de mensajes; vi) borrado rápido y código PIN de pánico (el usuario puede introducir un código PIN especial en la pantalla de bloqueo para borrar inmediatamente todos los datos del dispositivo), de igual forma, la introducción repetida de una contraseña incorrecta borraría todos los datos.

La comunicación solo era posible entre clientes de *EncroChat.* Estos teléfonos no se podían adquirir a través de canales de venta oficiales, sino que los vendedores los ofrecían en la plataforma eBay. Investigaciones posteriores revelaron que no se pudo identificar ninguna empresa legalmente establecida llamada *EncroChat,* y que estos dispositivos solo se vendían a personas seleccionadas, incluidos los

propios distribuidores. No se pudo identificar al responsable de *EncroChat,* ni la sede oficial de la empresa.

– La policía francesa consiguió, con la autorización de un juez, conservar datos de dicho servidor, en 2018 y 2019. Estos datos permitieron el desarrollo, por un equipo conjunto de investigación, que incluía expertos neerlandeses, de una aplicación informática de tipo «caballo de Troya».

– Dicha aplicación fue instalada en la primavera de 2020, con autorización del *Tribunal correctionnel de Lille* (Tribunal de lo Penal de Lille, Francia) en el citado servidor y, desde allí, en los mencionados teléfonos portátiles por medio de una actualización simulada.

– 32.477 usuarios, de un total de 66.134 registrados, distribuidos entre 122 países, se vieron, al parecer, afectados por la referida aplicación.

Sobre la información obtenida (algunas fuentes hablan de más de 100 millones de mensajes), Eurojust informó de su existencia a aquellos países cuyos nacionales operaban a través de *EncroChat*. En el caso de España, tras la tramitación de una Orden Europea de Investigación, la información se recibió en noviembre de 2020 y se incorporó a distintos procedimientos judiciales.

2. *Los datos de* EncroChat, *su incorporación al presente procedimiento y valor probatorio*

Los datos del servidor de *EncroChat* pueden plantear cuestiones de índole procesal en cada procedimiento penal en concreto, como son, entre otras: la manera de obtenerlos desde Francia, el que la técnica concretamente empleada para esta captación de datos no ha sido divulgada, por estar sujeta a secreto de defensa nacional conforme a tal normativa francesa (art. 4139 y 413-10 del CP francés.); la cadena de custodia del material aportado; la realización de copias; la extracción de datos relativos a personas, hechos y delitos específicos; su incorporación a cada procedimiento penal; o los informes policiales sobre la correspondencia entre *nicknames* e identidades de personas concretas.

Muchas de estas cuestiones deben ser observadas desde la perspectiva de cada procedimiento y la prueba practicada en cada uno de ellos; sin perjuicio de que, con carácter general, se pueda afirmar, como ya se ha indicado, que:

– Los datos se obtuvieron mediante la emisión de una OEI, por parte del Ministerio Fiscal, en las Diligencias de Investigación 20/2020.

– Se recogieron por parte de la fuerza policial española en dependencias policiales en Francia, en un disco duro, que quedó depositado en poder de la Guardia Civil.

– El Ministerio Fiscal autorizó a la Policía de Judicial para que: i) realizara una copia de la evidencia original, ii) analizara la información contenida en el citado disco duro, y iii) iniciara una investigación o aportara al proceso en curso la información obtenida.

Como se observa, los datos aportados por parte de Francia no son los datos originales del servidor, tal y como se obtuvieron, sino unos datos que fueron objeto de análisis y selección por las autoridades francesas, para discriminar cuáles podrían ser de interés para las autoridades españolas. Además, los datos que, en su caso, se incorporan a cada procedimiento penal en España, tampoco son los que se recibieron desde Francia; sino que, nuevamente, son datos que son objeto de análisis y selección, en este caso por parte de la Policía Judicial, para discriminar cuáles podrían ser de interés para cada procedimiento penal, en atención a las personas, hechos y delitos investigados.

Esta selección «en cascada» plantea el problema de las posibilidades para la defensa de impugnar la integridad y fiabilidad de los datos, porque nunca ha podido tener a su disposición los «datos en bruto».

2. PAUTAS JURISPRUDENCIALES Y DOCTRINA DEL TEDH

La sentencia examina la doctrina del TEDH y la propia jurisprudencia de la Sala, para apoyar su decisión, aunque no haya habido, con anterioridad, pronunciamientos específicos en relación a *EnchroChat.*

Y así, se citan sentencias del referido Tribunal Europeo sobre casos que guardan cierta similitud. Entre otras la STEDH (Gran sala), de 26 de septiembre de 2023, caso Yüksel Yalçinkaya c. Turquía (asunto núm. 15669/2020), que se refiere a otra red de mensajería encriptada, *ByLock.* Y la STEDH (Gran Sala), de 25 de mayo de 2021, caso Big Brother Watch y otros c. Reino Unido (asuntos núm. 58170/13, núm. 62322/14 y 24960/15) que examina un caso de interceptación masiva de comunicaciones transfronterizas *(bulk interception)* por parte de los servicios de inteligencia; así como del intercambio de la información obtenida entre Estados, cuya doctrina ha sido recogida ya por distintos pronunciamientos de la propia Sala Segunda.

Consecuencia de ello es que la jurisprudencia de la Sala, haciéndose eco de los pronunciamientos del TEDH, ha fijado las bases de una doctrina general sobre el acceso de la defensa a la totalidad del material inculpatorio, incluyendo –naturalmente– el supuesto de que tal material sea de naturaleza electrónica.

Entre dichas sentencias, se destacan la STS 993/2022, de 22 de diciembre, la STS 106/2023, de 16 de febrero, STS 873/2023, de 24 de noviembre y STS 902/2024, de 28 de octubre.

La STS 993/2022:

En relación al acceso de todo el material inculpatorio, efectivamente, tiene declarado el TEDH que el derecho a un juicio contradictorio exige, en un caso penal, que la acusación revele a la defensa todas las pruebas materiales que obren en su poder a favor o en contra del acusado (véase Edwards c. Reino Unido, 16 de diciembre de 1992, § 36, serie A núm. 247B, y Rowe y Davis, antes citada, § 60).

La expresión «prueba material» abarca todo el material en posesión de las autoridades con relevancia potencial, también si no se considera en absoluto, o no se considera relevante (compárese Edwards, citado anteriormente, § 36; Bendenoun c. Francia, 24 de febrero de 1994, § 52, serie A núm. 284; y Rowe y Davis, antes citada, § 60).

Y el hecho de no revelar a la defensa pruebas materiales que contengan datos que podrían permitir al acusado exonerarse o reducir su pena constituiría una denegación de las facilidades necesarias para la preparación de la defensa (véase Natunen c. Finlandia, núm. 21022/04, § 43, 31 de marzo de 2009; Matanoviæ, antes citada, § 157).

Preparación que requiere determinar si la cantidad de tiempo realmente disponible antes del final de la audiencia fue suficiente [Mattick, c. Alemania (dec.), núm. 62116/00, de 31 de marzo de 2005].

La STS 106/2023, de 16 de febrero, en la misma línea, afirmó:

«6. Para identificar cómo debe evaluarse si la persona acusada ha contado con las facilidades defensivas adecuadas que reclama el Convenio de 1950, resulta de extraordinario interés la STEDH, caso Rook c. Alemania, de 25 de octubre de 2019, en la que se abordan, precisamente, los problemas de acceso del demandante a una ingente información documental intervenida en el curso del proceso penal que se seguía en su contra, –nada menos que catorce millones de archivos electrónicos–, para cuyo examen, en parte, se requería, además, un muy costoso programa informático de lectura- y en qué medida ello pudo afectar a sus derechos defensivos.

Pues bien, «Para dicha evaluación, el Tribunal analizó los siguientes ítems: las condiciones en las que la persona acusada accedió al final de la investigación al expediente conformado por la acusación; si este contenía la información inculpatoria relevante; si dispuso del tiempo necesario para su examen; si existieron impedimentos graves para acceder al total de las informaciones intervenidas y almacenadas; si las modelizaciones o limitaciones de acceso fueron razonables; si se le prestó la ayuda o las facilidades que situacionalmente resultaban adecuadas para acceder al total o al máximo posible de los datos alma-

cenados; si se precisaron los documentos que prestaban soporte probatorio a la acusación y si se facilitó copia de los mismos al acusado –en el caso, se incluyeron en el expediente de acusación copias de veintiocho transcripciones de datos provenientes de la vigilancia de telecomunicaciones y alrededor de 1.100 impresiones de archivos electrónicos–; si se hizo algún uso de los datos o documentos intervenidos y no trasladados por copia a la defensa para formular acusación; si el tribunal hizo algún uso de datos para conformar su convicción que no constaban precisados en el expediente de acusación; si la parte que afirma haber sufrido el menoscabo ha identificado qué tipos de datos a los que no pudo acceder podrían tener potencial eficacia defensiva, atendiendo a que el propio investigado conocía los datos personales que fueron objeto de intervención».

Llegándose, en el caso, a la conclusión, de que no se vulneraron los derechos de defensa, pues el demandante contó con medios y tiempo suficiente para la adecuada y eficaz preparación de su defensa.

En cuanto a la STS 873/2023, de 24 de noviembre:

Se dice –con cita de STEDH, caso Rook c. Alemania, de 25 de octubre de 2019; STSS 507/2020, de 14 de octubre; 86/2022, de 31 de enero; 106/2023, de 16 de febrero– que en los casos de dificultades técnicas para el acceso a los datos, en particular cuando están encriptados, o los inconvenientes logísticos para su manejo y análisis cuando estos resultan muy voluminosos– es preciso activar salvaguardas específicas en orden a la recopilación y al tratamiento –*vid.* STS 425/2016, de 4 de febrero; Circular de la Fiscalía General del Estado 5/2019– pero también para la adecuada valoración de su fiabilidad. En particular, «en aquellos supuestos en los que los datos digitales se han obtenido sin control judicial posterior o no vienen acompañados de otras informaciones probatorias con potencial corroborativo –*vid.* sobre el uso probatorio de contenidos remitidos mediante servicios de mensajería, STEDH Yüksel Yalçinkaya c. Turquía, de 26 de septiembre de 2023–».

Y en cuanto a la STS 902/2024, de 28 de octubre:

El TEDH, tras recordar la doctrina de que las autoridades de la fiscalía deben revelar a la defensa todas las pruebas materiales que obren en su poder a favor o en contra del acusado, «El hecho de no comunicar a la defensa las pruebas materiales que contengan los datos que podrían permitir al acusado exonerarse a sí mismo o ver reducida su condena constituiría una denegación de las facilidades necesarias para la preparación de la defensa (véase Natunen c. Finlandia, n. 21022/04, § 43, de 31 de marzo de 2009; Matanoviæ c. Croatia, n. 2742/12, de 4 de abril de 2017, § 157)».

La doctrina expuesta ha configurado «un cuerpo de doctrina» que ha sido reiterado en otras, como la STS 37/2025, de 23 de enero, que reproduce la contenida en la STS 106/2023, de 16 de febrero.

Además de dicha doctrina general, es de cita obligada la ya citada STEDH (Gran sala), de 26 de septiembre de 2023, caso Yüksel Yalçinkaya c. Turquía (asunto núm. 15669/2020) que aborda la posibilidad de acceso de la defensa a la totalidad de los «datos en bruto» obtenidos del servidor de una aplicación encriptada de mensajería, denominada ByLock.

De la misma –continúa la sentencia de pleno–, se pueden extraer los criterios siguientes sobre la cuestión examinada:

«1. Lo relevante es que, si la equidad general del proceso se garantizó, desde la perspectiva de las garantías procesales e institucionales y los principios fundamentales de un juicio justo inherentes al artículo 6 CEDH (ap. 313).

2. Se debe evaluar si se dio a la defensa la oportunidad de impugnar las pruebas y de oponerse a su uso, en circunstancias en las que se respetaron los principios del procedimiento contradictorio y de igualdad de armas entre la acusación y la defensa (ap. 324).

3. El hecho de que existan informes (periciales, policiales…) sobre los datos en el procedimiento y que la defensa tenga pleno acceso a los mismos no es obstáculo o excusa para negar su derecho o interés en solicitar el acceso a los datos del servidor o del dispositivo electrónico, a partir de los cuales se han elaborado dichos informes (ap. 327).

4. La necesidad de revelar a la defensa "todas las pruebas materiales" no puede limitarse a las pruebas consideradas pertinentes por la acusación; sino que abarca todo el material en posesión de las autoridades que pueda ser pertinente para la defensa.

5. Sin perjuicio de ello, el derecho de la defensa a la exhibición de pruebas se puede limitar por diversas razones, entre ellas que las pruebas que obran en poder de la acusación se refieran a una gran masa de información electrónica, de modo que puede que no sea posible, o incluso necesario, revelar esa información a la defensa en su totalidad.

6. El derecho de la defensa a la exhibición de pruebas no se debe confundir con el derecho de acceso a todo ese material o información.

7. Si ello es así, lo determinante es valorar si el eventual perjuicio sufrido por la defensa, debido a la no divulgación de los datos del servidor, se vio contrarrestado por garantías procesales adecuadas y si se le dio la debida oportunidad de preparar su defensa, como exige el artículo 6 CEDH.

8. Ello exige valorar circunstancias como las siguientes:

1.1) Respecto a la posible solicitud de incorporación de los "datos en bruto" al proceso: i) si se contestó o no a la misma; y ii) en el caso de que se contestara, cuáles fueron las razones esgrimidas para la denegación.

1.2) Respecto a la posible solicitud de que los "datos en bruto" se sometan a un examen independiente, deben valorarse los mismos extremos, si bien teniendo en cuenta que: i) la solicitud de un examen independiente no impone a los tribunales nacionales la obligación de ordenar que se emita un dictamen pericial o que se adopte cualquier otra medida de investigación, por el mero hecho de que una de las partes lo solicite; y ii) el hecho de que los tribunales nacionales se basen exclusivamente en la información y los informes proporcionados por autoridades estatales para determinar la culpabilidad del demandante, sin someter los "datos en bruto" a un examen directo, no basta por sí solo para declarar injusto el procedimiento, habida cuenta, en particular, de las competencias técnicas requeridas para examinar los datos en su forma bruta.

1.3) Esta valoración debe ser especialmente cautelosa cuando concurren determinadas circunstancias como, por ejemplo, cuando: i) los datos han sido "procesados" por distintas autoridades y con distintos fines (como fines de inteligencia o como prueba penal para iniciar investigaciones y detener a los sospechosos); ii) existen elementos en el informe o los distintos informes obrantes en el procedimiento que introduzcan alguna duda o contradicción sobre la integridad o fiabilidad de los datos; iii) el pleno acceso de la defensa al material puede servir para reforzar sustancialmente su pretensión o sus argumentos; y iv) los datos tienen un "peso preponderante" como indicio o prueba en su contra».

Es decir –concluye en este punto, la sentencia–, **no es posible un análisis general acerca del valor probatorio de los datos procedentes de *EncroChat*, alejado de los pormenores de cada caso concreto**.

Por eso, «Hemos de ceñirnos al caso que concentra nuestra atención».

3. VALORACIÓN Y APLICACIÓN DEL MATERIAL OBTENIDO, EN EL PRESENTE CASO

Concluye la sentencia de pleno, examinando las quejas de la defensa respecto al valor probatorio de las conversaciones de *Encrochat,* incluso las que aluden a la regularidad de su obtención.

Y se inicia el análisis, reprochando a los Letrados que, en los recursos en cuestión, están enunciadas en términos genéricos ya que, por ejemplo, no inciden en la cadena de custodia, en la transmisión de datos en bruto.

Se centran en denunciar su vinculación con una «investigación prospectiva», como «idea fuerza», aunque lo que si cuestionan es la asignación de las identidades a los *nicknames* con el que operan en la red encriptada, al menos tres de los recurrentes.

La sentencia de Pleno manifiesta que, en el caso, la incorporación a la causa de los elementos obtenidos de la interceptación de la red *EnchroChat* tuvo lugar cuanto la instrucción estaba ya muy avanzada, y que las pruebas de cargo derivaban esencialmente de los previos seguimientos, una vez ratificados por los agentes que los realizaron, y en los hallazgos obtenidos en dichos recursos, con lo que la incidencia de los aludidos datos goza de un valor meramente corroborador.

Además, la incorporación de ese material documental se realizó mediante un documento firmado digitalmente compuesto por un total de 867 páginas numeradas y con marca de agua, con lo que el órgano de enjuiciamiento entendió que ello «garantiza la inalterabilidad y fidelidad de los datos concretos extraídos de la copia forense y facilitados a esta Unidad sobre la base del citado Decreto de la Fiscalía Especial Antidroga de la Audiencia Nacional». Decisión avalada por la Sala de apelación.

Así, con todo detenimiento, lo explicó la sentencia de la Sala de lo Penal de la Audiencia Nacional:

«De las gestiones practicadas por esta Instrucción (JCI núm. 1 de la AN), se tiene conocimiento de que con fecha 18 de noviembre de 2020, la Fiscalía Especial Antidroga de la Audiencia Nacional, mediante las Diligencias de Investigación 20/2020, autorizó a la Unidad Técnica de Policía Judicial (UTPJ), junto con el Grupo de Informática Forense de la Jefatura de Información de la Guardia Civil, realizaran una copia forense de las evidencias legales obtenidas del servidor de dicho servidor sito en Francia. Citadas diligencias de investigación dimanan de las Di. 16/2020 que se incoaran como consecuencia de la comunicación efectuada por las Autoridades Judiciales de Lille (Francia), referida a un sistema de encriptación de comunicaciones telefónicas conocido como "encrochat" en que se transmitía una información de actividades criminales supuestamente cometidas en España. 1 W Que teniendo conocimiento de que, junto a las actividades objeto de las D.1. 1612020, las intervenciones de las comunicaciones obtenidas del servidor de Encrochat sito en Francia podrían referirse a actividades delictivas, se remitió el 23 de julio de 2020 una Orden Europea de Investigación (OEI), cuyo objeto era obtener todos los datos de comunicación y asociados referentes a España, desde el inicio de la intervención del servidor Encrochat hasta su finalización.

Dicha OEI fue cumplimentada por comunicación de la Autoridad judicial de Lille, de 14 de septiembre de 2020, que expresamente

autoriza a la Fiscalía Antidroga a la utilización de los datos transmitidos en el marco de la solicitud de asistencia judicial, de modo que puede implementarse en toda investigación y en virtud de cualquier procedimiento judicial, actuaciones judiciales, instrucción o juicio. Así mismo, en las D. I 20/2020, el Fiscal Jefe de la Fiscalía Especial Antidroga de la Audiencia Nacional acuerda que, realizaran una copia forense de la evidencia original, manteniendo la inalterabilidad de ésta, quedando como depositarios de las evidencias legales referidas en el Decreto de 18 de noviembre de 2020, emitido por el Fiscal Jefe de la Fiscalía Especial Antidroga de la Audiencia Nacional.

En el referido documento, el Fiscal Jefe de la Fiscalía Especial Antidroga autoriza a las Unidades con funciones de Policía Judicial de la Guardia Civil, a realizar el análisis de la información contenida en el citado duro, para tratar de determinar: a) Si contienen elementos suficientes para iniciar una investigación. b) Si están relacionadas con una investigación ya iniciada; y, caso de resultar positiva, si la evidencia analizada, en relación con la investigación, aporta algún dato relevante.

En virtud de lo anterior, dicha UTPJ emitió oficio de fecha 25 de febrero de 2021, adjunta en un documento firmado digitalmente compuesto por un total de 867 páginas numeradas y con marca de agua NUM086, los datos relativos a las comunicaciones de los usuarios "Palillo", "Rubia", "Flaca", "Pelirojo" y "Perico", que garantiza la inalterabilidad y fidelidad de los datos concretos extraídos de la copia forense y facilitados a ésta Unidad (UOPJ Barcelona) sobre la base del citado Decreto de la Fiscalía Especial Antidroga de la Audiencia Nacional».

A partir de dichos datos, agentes de la Guardia Civil realizaron minuciosos informes individualizados por cada uno de los usuarios de los *nicknames* identificados en esta causa, que analizan las distintas conversaciones y explican que establecen la conexión con los investigados a partir de los posicionamientos en los repetidores en red desde los que se ha conectado cada uno; del análisis de los mensajes encriptados que se intercambiaban, y su contraste con los datos que la investigación llevada a cabo hasta ese momento había arrojado.

Unos informes que fueron ratificados en el acto de juicio, con sometimiento de sus autores al interrogatorio contradictorio, y respecto de los que, pese a tener acceso a los mismos desde que se levantó el secreto de las actuaciones, no consta, al menos los recursos no lo identifican, petición alguna orientada a obtener mayor información respecto de los mismos, o tratar de contradecir sus conclusiones con otros medios de prueba.

En esas condiciones –se concluye– el valor probatorio que se les ha otorgado encuentra pleno acomodo en los parámetros que nuestra jurisprudencia, seguidora a su vez de las pautas marcadas por el TEDH, ha descrito».