El asunto Encrochat y la prueba transnacional europea. Matización de las garantías procesales

The EncroChat Case and European Cross-Border Evidence. Nuancing Procedural Safeguards

Dr. Luis Aparicio Díaz
España
Montero-Aramburu
& Gómez-Villares Atencia.
Universidad Loyola de Andalucía
lad@monteroaramburugva.com
laparicio@uloyola.es
ORCID: 0000-0001-8607-4921

Resumen

Este trabajo pretende examinar, sin ánimo de exhaustividad, la problemática derivada de la utilización en el proceso penal español de las evidencias obtenidas a partir de la extraordinaria intervención tecnológica realizada por las autoridades francesas y holandesas en la red Encrochat.

Se analiza el status jurídico de la prueba cuando fue obtenida por las mencionadas autoridades nacionales, su transmisión mediante instrumentos de cooperación judicial europea y, finalmente, la incorporación de dicha prueba a los procedimientos judiciales españoles.

El análisis se realiza teniendo en cuenta las fuentes abiertas de carácter policial que se refieren al asunto Encrochat, la normativa española y europea y la jurisprudencia relativa al asunto, tanto del Tribunal de Justicia de la Unión Europea, como también de nuestro Tribunal Supremo, con especial mención de la doctrina relativa a la Orden Europea de Investigación.

El trabajo incide en los problemas derivados de la admisibilidad de la prueba tanto en relación con su obtención en la intervención tecnológica como también a su transmisión a las autoridades españolas desde Francia, así como a los problemas procesales derivados (contradicción efectiva, autenticidad del material, integridad del soporte material e imputación subjetiva del material probatorio).

Abstract

This paper aims to examine, without seeking to be exhaustive, the legal challenges arising from the use in Spanish criminal proceedings of evidence obtained through the extraordinary technological intervention carried out by French and Dutch authorities on the EncroChat network.

The study analyzes the legal status of the evidence at the time of its collection by the aforementioned national authorities, its transmission via European judicial cooperation instruments, and, ultimately, its admissibility and incorporation into Spanish judicial proceedings.

The analysis is conducted by taking into account open-source law enforcement data regarding the EncroChat case, Spanish and European regulations, and relevant case law from both the Court of Justice of the European Union (CJEU) and the Spanish Supreme Court, with particular emphasis on the doctrine surrounding the European Investigation Order (EIO).

The paper focuses on the issues stemming from the admissibility of evidence, both in relation to its initial seizure through technological intervention and its subsequent transfer to Spanish authorities from France. It further addresses the resulting procedural challenges, including effective cross-examination (*contradicción efectiva*), the authenticity of the material, the integrity of the physical or digital media, and the subjective attribution of the evidentiary material to the defendants.

Palabras Clave

EncroChat, Orden Europea de Investigación, prueba transnacional, garantías procesales, Intervención tecnológica

Key Words

EncroChat, European Investigation Order, Cross-border evidence, Procedural safeguards, Technological intervention

Introducción, objetivo y metodología

La globalización de las relaciones económicas y sociales como realidad bien implantada ya en los albores del siglo XXI determina con claridad el papel central de la prueba transnacional en procedimientos penales de cierta complejidad en tramas internacionales vinculadas, habitualmente, a delitos graves. El instituto procesal de la prueba, bien cuajado hasta hace poco tiempo, se resquebraja y pide ser reelaborado en un entorno que pugna con su vigencia: el recurso de las tramas internacionales a los sistemas informáticos, la digitalización, el uso de infraestructuras tecnológicas deslocalizadas han erosionado el uso de las categorías consolidadas sobre la prueba. No ya sólo sobre la configuración de la prueba obtenida en territorio nacional y la obtenida fuera de nuestras fronteras, sino también sobre las mismas garantías del instituto probatorio. El asunto Encrochat, como antes lo fue la famosa "lista Falciani" suponen un punto de inflexión de lo que será común en la era del big data: la obtención de prueba tecnológica que implicará la captación masiva de datos, la técnica de investigación digital invasiva, la transferencia internacional de resultados, su utilización por parte de jurisdicciones de distintos países y una necesaria reelaboración, o cuando menos una actualización, respecto de la suficiencia de las garantías procesales en el marco de un estado democrático y de derecho. La metodología ha consistido en el análisis de fuentes abiertas de órganos policiales europeos así como el análisis en profundidad de la Sentencia del Tribunal Supremo 854/2025.

1.- ¿QUÉ ES ENCROCHAT?

Según refiere Europol,[1] Encrochat era una red telefónica encriptada en la que se ofrecían a los clientes teléfonos que garantizaban un anonimato total. No se asociaban a dispositivos ni a tarjetas SIM en la cuenta del cliente y su adquisición se llevaba a cabo en condiciones que garantizaban su imposible trazabilidad. Además, se garantizaba también una discreción absoluta tanto respecto de la interfaz encriptada) sistema operativo dual, la interfaz encriptada oculta para no ser detectable), como también del propio terminal, al que se le extraían la cámara, el micrófono, el GPS y el puerto USB.

Junto con estas garantías también se incluían funciones destinadas a garantizar la "autodestrucción" de sus propios contenidos. Y así, incluía la eliminación automática de mensajes en los terminales de sus destinatarios, código PIN específico destinado a la eliminación inmediata de todos los datos del dispositivo (algo así como un botón del pánico) y la eliminación de todos los datos en caso de entradas consecutivas de una contraseña incorrecta. Funciones desarrolladas, aparentemente, para permitir borrar rápidamente los mensajes del dispositivo en caso de emergencia. Incluso se ofrecía el borrado del dispositivo a distancia por parte del servicio de asistencia.

Estos "criptoteléfonos" fueron vendidos por Encrochat a un coste aproximado de 1.000 de mil Euros cada uno a escala internacional y ofrecía suscripciones con cobertura mundial al coste de unos mil quinientos euros semestrales, con soporte las 24 horas todos los días del año.

2.- CRONOLOGÍA DE LA INTERVENCIÓN.

De acuerdo con Eurojust,[2] el Departamento de Informática Electrónica (INL) del Instituto de Investigación Criminal de la Gendarmería Nacional francesa (IRCGN) detectó en 2017 el uso de los teléfonos que utilizaban el sistema de comunicación segura EncroChat, y decidió iniciar una profunda investigación de estos teléfonos y su sistema de encriptado para poder comprender su funcionamiento.

El 15 de noviembre 2018 se abrió una investigación preliminar por parte del del Centro de Lucha contra el Crimen Digital de la Gendarmería francesa (C3N) llevándose a cabo las primeras investigaciones técnicas.

Fruto de aquellas primeras investigaciones, el día 7 de diciembre de 2018 la Jurisdicción Interregional Especializada (JIRS) de Lille abrió a su vez una investigación sobre Encrochat por los delitos de asociación de malhechores para cometer delitos castigados con al menos diez años de prisión y provisión, transferencia e importación de medios de criptología sin declaración previa.

Los Tribunales Interregionales Especializados (JIRS) fueron creados por la Ley nº 2004-204 de 9 de marzo de 2004 que adapta el sistema judicial a los cam-

1 Europol. (2020, July 2). Dismantling of encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

2 Eurojust. (2020, July 2). EncroChat investigation in France [PDF]. https://www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_EncroChat-investigation-in-France_FR.pdf

bios en la delincuencia, conocida como "Perben II", y desempeñan un papel clave en el combate del crimen organizado. Este sistema se implementa en ocho tribunales judiciales: Burdeos, Lille, Lyon, Marsella, Nancy, París, Rennes y Fort-de-France. Cada tribunal especializado cuenta con una sección de la fiscalía, y centros de investigación propios. No constituyen un nuevo orden judicial, sino que se crean como secciones especializadas dentro de tribunales ordinarios para dar respuesta a fenómenos criminales de especial complejidad.

El JIRS de Lille asumió esta investigación debido a la localización en su demarcación de los servidores de Encrochat, que según la Sentencia del Tribunal Supremo núm. 854/2025 de 16 de octubre se encontraban en la localidad de Roubaix.

A principios de 2019, el proyecto CERBERUS, dirigido por la Gendarmería francesa y financiado con fondos europeos, permitió acelerar las investigaciones sobre estos teléfonos. Tanto la Gendarmería francesa como las investigaciones en curso demostraron la aparición recurrente de estos criptoteléfonos en casos de transporte y tráfico de drogas relacionados con el crimen organizado. Y las investigaciones técnicas realizadas por la misma Gendarmería permitió concluir que si bien esta solución de comunicación cifrada no estaba declarada en Francia, sí operaba desde servidores instalados en territorio francés (Roubaix) dando soporte a clientes internacionales.

De acuerdo con la Sentencia del Tribunal Supremo 854/2025, las operaciones tecnológicas fueron autorizadas por autos de 30 de enero de 2020, 12 de febrero de 2020, 4 de marzo de 20 de marzo de 2020 y 31 de marzo de 2020, a instancia del IImo. Sr. Fiscal de la República.

Según Europol,[3] fueron las autoridades francesas las que decidieron abrir un caso en Eurojust, la Agencia de Cooperación Judicial Penal de la UE, hacia los Países Bajos en 2019. Razón por la que la Sentencia 854/2025 antes citada refiere que fue un equipo conjunto formado por franceses y holandeses quienes, en fecha desconocida, pero en todo caso durante la primavera de 2020, infectaron el sistema Encrochat con una aplicación informática tipo "caballo de Troya" al que Europol se refiere eufemísticamente como "dispositivo técnico".[4] Un "troyano" que permitió a las autoridades examinar todas las comunicaciones vía Encrochat sin que sus usuarios pudieran advertirlo hasta la noche del 12 al 13 de junio de 2020, en que EncroChat emitió una alerta de seguridad a sus clientes indicando que la solución había sido víctima de una "intervención ilegal" por parte de "entidades gubernamentales". Se les aconsejaba apagar y deshacerse físicamente de sus dispositivos ("You are advised to

3 Europol. (2020, July 2). Dismantling of encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

4 Europol. (2023, July 5). Dismantling encrypted criminal EncroChat communications leads to over 6,500 arrests and close to EUR 900 million seized. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized

power off and physically dispose your device immediately").[5]

Mientras se estaban llevando a cabo la interceptación de estas comunicaciones, el 15 de marzo de 2020, la Subdirección de Policía Judicial (SDPJ) creó una unidad nacional de investigación en el C3N de Pontoise, con un puesto de mando y varios grupos de investigación. La operación se denominó EMMA 95 y fue reforzada por investigadores de las secciones de investigación y de las oficinas centrales, contando con más de 60 gendarmes dedicados exclusivamente al uso de datos. Por su parte, en Holanda, la operación fue conocida como LEMONT.[6]

El día 10 de abril de 2020 se formó un Equipo Conjunto de Investigación (ECI) entre Francia y Países Bajos, bajo EUROJUST y con apoyo de EUROPOL.

El día 28 de mayo de 2020 se abrió la investigación judicial confiada a la Dirección General de la Gendarmería Nacional y al ya referido C3N por los delitos de asociación de malhechores para preparar delitos graves, incluyendo tráfico de drogas, blanqueo agravado, tenencia y tráfico de armas; blanqueo en banda organizada y provisión, transferencia e importación de medios de criptología sin declaración previa.

Los investigadores policiales lograron interceptar, compartir y analizar más de 115 millones de conversaciones mantenidas por un número estimado de más de 60 000 usuarios.

3.- La infección con un virus troyano como medio de investigación

La captación de datos informáticos, como es la infección de un sistema como un virus, es una técnica de investigación prevista por el derecho francés de acuerdo con lo previsto en el Título XXV del Código de Procedimiento Penal, bajo la rúbrica *Procedimiento aplicable al crimen organizado y a la delincuencia y delitos*. En concreto, dentro de la Sección 6 rubricada *Otras técnicas especiales de investigación*, que recoge en su Párrafo 4 la rúbrica *Captura de Datos informáticos* que contiene los artículos 706-102-1 a

El artículo 706-102-1 (derogado, por cierto, por la Ordenanza nº 2025-1091 de 19 de noviembre de 2025 - art. 1 (V) a partir de 1 de enero de 2029) refiere que se

Se puede recurrir a la instalación de un dispositivo técnico con el propósito, sin el consentimiento de las partes interesadas, de acceder, grabar, almacenar y transmitir datos informáticos en cualquier lugar, tal y como se muestran en una pantalla para el usuario de un sistema automatizado de procesamiento de datos, ya que los introduce introduciendo caracteres o a medida que son recibidos y emitidos por los periféricos.

Dentro de ese mismo párrafo, el art. 706-102-3 condiciona la decisión que autorice el uso del mecanismo antes indicado, bajo pena de nulidad, a la especificación del delito que justifica di-

5 Eurojust. (2020, July 2). EncroChat investigation in France [PDF]. https://www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_EncroChat-investigation-in-France_FR.pdf

6 Europol. (2020, July 2). Dismantling of encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

cha operación, así como la duración de la misma.

Finalmente, el art. 706-102-3 se refiere a determinados extremos que resultan necesario para la efectiva instalación del dispositivo tecnológico que implican, lógicamente, actuaciones materiales sobre realidades físicas tangibles. En esencial, el legislador francés permite, con autorización judicial, la entrada a un vehículo o a un lugar privado sin el conocimiento o consentimiento del propietario o poseedor del vehículo, del ocupante del local o de cualquier persona titular de un derecho sobre él. Operaciones materiales que sólo pueden tener el propósito de implementar el dispositivo técnico. Lógicamente, esta habilitación legal se extiende, también, a la implementación de las operaciones destinadas a la retirada del dispositivo técnico que se hubiere instalado previamente.

El legislador francés también permite al Juez autorizar la transmisión del dispositivo a través de una red de comunicaciones electrónicas, bajo la autoridad y supervisión judicial. Como en el caso anterior, también se podrá llevar a cabo dicha operativa para la retirada del dispositivo técnico que se hubiere instalado.

Haciendo uso, pues, de dicha habilitación legal, las autoridades francesas lograron infectar con un virus informático la red Encrochat. En relación con el dicho procedimiento francés, el Tribunal Supremo español, en su Sentencia 854/2025 añade también que el ordenamiento jurídico francés cuenta con una norma que regula los medios o mecanismos de encriptación. Se trata de la *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*.

Tal norma parte del principio de que el objetivo principal de los métodos criptológicos es garantizar la seguridad del almacenamiento o transmisión de datos, garantizando su confidencialidad, autenticación o el control de su integridad (art. 29); de manera que su uso es libre y lícito y lo es también el suministro, la transferencia desde o hacia un Estado miembro de la Unión Europea, o la importación y la exportación de medios criptográficos que proporcionen exclusivamente funciones de autenticación o control de integridad (art. 30).

Sin embargo, cuando se trate de un medio que no preste exclusivamente funciones de autenticación o control de la integridad, es preciso cumplir una serie de presupuestos:

1) Las operaciones de suministro, transferencia desde un Estado miembro de la Unión Europea o importación de tal medio de criptología quedan sujetas a una declaración previa al Primer Ministro, poniendo a su disposición una descripción de las características técnicas del medio, así como el código fuente del software utilizado (art. 30.III).

2) Las operaciones de transferencia a un Estado miembro de la Unión Europea y la exportación de tal medio de criptología estarán sujetas a la autorización del Primer Ministro (art. 30.IV).

3) También se debe declarar la prestación de servicios de criptología (art. 31).

En consecuencia, la ley citada establece como punibles penalmente las conductas siguientes:

1) El incumplimiento de la obligación de declarar prevista anteriormente (artículo 35.I.1).

2) El hecho de exportar un medio de criptología o de transferirlo a un Estado miembro de la Unión Europea, sin haber obtenido previamente la autorización prevista anteriormente (art. 35.I.2)

3) El acto de vender o alquilar un medio de criptología que haya sido objeto de una prohibición administrativa de circulación (art. 35.III).

4) El hecho de prestar servicios de criptología, destinados a garantizar funciones de confidencialidad, sin haber cumplido con la obligación de declarar prevista anteriormente (art. 35. IV).

4.- La llegada de la información a España: la Orden Europea de Investigación

Siguiendo la ya citada Sentencia del Tribunal Supremo 854/2025, fue la Fiscalía de Lille la que transmitió información general, espontáneamente, a la Unidad de Criminalidad Informática de la Fiscalía General del Estado, sobre la operación en la que habían sido incautados datos de usuarios españoles implicados en delitos de tráfico de drogas en España.

La Fiscalía General del Estado, a su vez, remitió esta información a la Fiscalía Especial Antidroga que, en un primer momento las incorporó a las ya existentes Diligencias de Investigación 16/20 (seguidas por un delito de blanqueo contra los resellers de los terminales de *EncroChat)*. Se incorporaron a esas diligencias por la sola mención de *EncroChat,* pero una vez traducido el documento francés, el Fiscal jefe de la FEAD advirtió la relevancia de la información, que desbordaba por completo dicho procedimiento. De ahí que se desglosara ese informe y se incoaran las Diligencias de Investigación 20/20, el 23 de julio de 2020, emitiendo ese mismo día Orden Europea de Investigación para obtener la información que los franceses ofrecían en la información espontánea.

Cabe recordar que fue la Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014 la que regula la orden europea de investigación en materia penal, transpuesta al Derecho español por la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación. Gracias a este nuevo instrumento, se creó un sistema general para obtener pruebas en los casos de dimensión transfronteriza, basado en el principio de reconocimiento mutuo, pero que tenga también en cuenta la flexibilidad del sistema tradicional de asistencia judicial. De acuerdo con su art. 1.1, una OEI se puede emitir, bien para la ejecución de una o varias medidas de investigación específicas en otro Estado miembro, con vistas a obtener pruebas; o para la obtención de pruebas que ya obren en poder de las autoridades competentes del Estado de ejecución; es decir, para la transmisión de dichas pruebas a las autoridades competentes del Estado de emisión. El caso Encrochat se encuentra en este segundo caso.

El Fiscal Jefe de la Fiscalía Especial Antidroga dictó Decreto, de fecha 18 de noviembre de 2020, en las Diligencias de Investigación 20/2020, en el que se describe el *iter* que se siguió para la obtención de los datos de *EncroChat:*

1. Las Diligencias de Investigación 20/2020 dimanan de las Diligencias de Investigación 16/2020, que se incoaron como consecuencia de la comunicación efectuada por las autoridades francesas, referida a un sistema de encriptación de comunicaciones telefónicas, conocido como *EncroChat,* en la que transmitía información sobre actividades criminales supuestamente cometidas en España (esencialmente, la comercialización de terminales de comunicación).

2. Como las intervenciones de las comunicaciones obtenidas del servidor sito en Francia podrían referirse a actividades de tráfico de drogas, se optó por remitir, 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. Concretamente, en la OEI se hacía constar lo siguiente:

   2.1 En la "Sección C: Medida o medidas de investigación de deben realizarse", la medida se describe de la siguiente manera:

   "Se requiere de la Autoridad Judicial francesa que facilite los datos almacenados en los servidores de EncroChat intervenidos en virtud de la medida judicial autorizada en su procedimiento en curso por la investigación de la Organización EncroChat, debido a que pudieran contener información de relevancia sobre diferentes aspectos relacionados con la actividad de blanqueo de capitales investigada por la autoridad española, desarrollada supuestamente por la referida Organización en España, así como por la red de distribuidores y revendedores de dicha tecnología en ese territorio.

   En concreto se solicitan todos los datos asociados a los usuarios de este sistema de comunicación encriptado EncroChat que se hallen registrados en el territorio nacional de España, tales como: identificación del usuario, nombre de usuario, número de IMEI, número de IMSI, alias, contraseña, red telefónica operadora, datos asociados a comunicaciones mediante llamadas de voz, datos asociados a comunicaciones mediante mensajería escrita, notas, datos asociados a contactos, listado de llamadas, datos de geolocalización y conexiones asociadas al tráfico de datos, comentarios, redes Wifi usadas, calendario, así como cualquier otro dato disponible.

   Respecto al alcance temporal de los datos, se solicitan los datos correspondientes desde la fecha de inicio de la intervención del servidor EncroChat hasta la fecha de finalización de dicha medida.

   Asimismo, se solicita que se autorice el uso de estos datos como pruebas válidas en un procedimiento judicial español".

   En la casilla correspondiente se marcó la opción "Obtención de información o de pruebas que ya están en posesión de la autoridad de ejecución".

2.2 En la "Sección G: Motivos de la emisión de la OEI", los hechos que justifican la orden son los siguientes:

"A) Se siguen en esta Fiscalía Especial Antidroga de la Audiencia Nacional diligencias por la presunta comisión de un delito de blanqueo de capitales, existiendo indicios racionales de criminalidad del establecimiento de una red de blanqueo de capitales liderada en España por J. A. C. la cual, valiéndose de un entramado societario sustentado en la estructura de la tecnología EncroChat creado para facilitar la comisión del delito, procede al blanqueo de dinero procedente de diferentes delitos, principalmente tráfico de drogas, mediante la fabricación, venta, distribución y prestación de servicios de tecnología de comunicación encriptada EncroChat sufragada por sus clientes mediante dinero de ilícita procedencia.

Asimismo, se tiene constancia de la existencia de una red de distribuidores y revendedores de tecnología EncroChat en España, que igualmente blanquearían el beneficio de su propia actividad criminal, así como la de personas dedicadas a la comisión de delitos, mediante la venta de dispositivos de comunicación y prestación de servicios EncroChat sufragados con dinero de ilícita procedencia, conformando una segunda red en España dedicada a la comisión del delito investigado.

Consecuentemente, a la vista de la información remitida por la Jurisdicción interregional Especializada (JIRS) de Lille a esta Instrucción referente a las comunicaciones y datos obrantes en la intervención del servidor informático de EncroChat realizada en la investigación seguida por esa Autoridad judicial francesa, esta aportación de datos podría ofrecer indicios acerca de los siguientes aspectos de interés para la presente investigación:

— Definición del rol, cometidos y operativas desarrolladas por las personas físicas y jurídicas investigadas en el seno de la Organización EncroChat en su rama española, principalmente J. A. C. y su entorno.

— Identificación de la red de distribuidores y revendedores presentes en España.

— Operativas de blanqueo de capitales llevadas a cabo por los integrantes de la Organización EncroChat.

— Operativas de blanqueo de capitales llevadas a cabo por la red de distribuidores y revendedores en España.

— Conocimiento por parte de los vendedores del origen ilícito del dinero recibido como contraprestación a la venta de tecnología EncroChat a su red clientelar.

B) Por información policial se tiene conocimiento que de los datos almacenados en los servidores de EncroChat se deriva-

ría importante información en relación con delitos de tráfico de drogas vinculados con territorio español, por lo que se incoan las presentes diligencias, en el contexto de las cuales se emite la presente OEI".

Igualmente, en la misma Sección G, en el apartado relativo a la naturaleza y tipificación jurídica del delito o delitos para los que se emite la OEI y norma legal aplicable, se indica:

"La presente OEI se emite para la investigación de un delito tráfico de drogas, blanqueo de capitales procedentes del narcotráfico, cometido por organización internacional de carácter criminal, todo ello tipificado en los artículos 301, 302, 303 (blanqueo), 368, 369, 369 bis (tráfico de drogas), 570 bis (organización criminal), todos ellos del del Código Penal español".

1. Dicha OEI fue cumplimentada por comunicación de la autoridad judicial de Lille, de 14 de septiembre de 2020, que expresamente autorizó a la Fiscalía Antidroga para la utilización de los datos transmitidos en el marco de la presente solicitud de asistencia judicial, de modo que puede implementarse en toda investigación y en virtud de cualquier procedimiento judicial, actuaciones judiciales, instrucción o juicio.

2. Por Decreto de 10 de noviembre de 2020, se autorizó a que un teniente de la Unidad Central Operativa (UCO) de la Guardia Civil se desplazara a Francia, para la transmisión efectiva de los datos objeto de la OEI citada.

3. El 12 de noviembre de 2020, se produjo la entrega, en dependencias policiales en Francia, de un disco duro conteniendo los datos.

4. Una vez en España, la Fiscalía Antidroga acordó lo siguiente:

- Que el disco duro quedará depositado, de forma segura, en las dependencias de la Unidad Central Operativa de la Guardia Civil, o en donde se determine por la Jefatura de policía Judicial de la Guardia Civil.
- Autorizar a la Unidad Técnica de Policía de Judicial, en conjunción con el Grupo de Informática Forense de la Jefatura de Información de la Guardia Civil, a la realización de una copia forense de la evidencia original, manteniendo la inalterabilidad de ésta, con el objetivo de realizar un procesamiento de los datos que permita su correcta visualización.
- Autorizar a las Unidades con funciones de Policía Judicial de la Guardia Civil, a realizar el análisis de la información contenida en el citado disco duro, para tratar de determinar: i) si contienen elementos suficientes para iniciar una investigación; y ii) si están relacionadas con una investigación ya iniciada y, en caso de ser así, si la evidencia

analizada aporta algún dato relevante.

- Autorizar a las Unidades con funciones de Policía Judicial de la Guardia Civil, bien a iniciar una investigación, en el primer caso; bien a aportar al proceso la información complementaria obtenida, en el segundo caso, para que se valore por el Juez de Instrucción y el Ministerio Fiscal. En ambos casos, para que la información se pueda integrar en un proceso penal, deberá ir acompañada de un oficio de remisión, emitido por la Unidad Técnica de Policía Judicial de la Guardia Civil, aportando los datos concretos extraídos de la copia forense, con la garantía de su inalterabilidad.

5.- Cuestiones procesales suscitadas respecto de la Orden Europea de Investigación que permitió la llegada a España de la información francesa

5.1.- La Fiscalía como autoridad de emisión de la Orden Europea de Investigación

Se ha discutido la posibilidad de que el Ministerio Fiscal fuera la autoridad para emitir la Orden Europea de Información. Posibilidad que no ofrece dudas, a juicio del Tribunal Supremo, en la medida en que, en opinión de la Sala, puede ordenar la transmisión de pruebas de un procedimiento interno a otro.

Se invoca la Sentencia del TJUE de 30.04.2024 (Asunto M.N.) C-670/22, conforme a la cual la transmisión de pruebas no debe ser necesariamente acordada por un Juez cuando en virtud del derecho interno la transmisión de esa prueba puede ser ordenada por un fiscal.

Esta posibilidad se residencia por el Tribunal Supremo en el art. 588 bis LECrim, que a su vez reenvía al tenor del art. 579 bis de la ley rituaria y en lo dispuesto en el Pleno No Jurisdiccional de la Sala de lo Penal del día 26.05.2009 cuyo asunto se refería a la habilitación de escuchas telefónicas procedentes de diligencias distintas las que corresponden al juicio. Cuestión ya de por sí llamativa, toda vez que al tiempo de dictarse ese acuerdo No Jurisdiccional del Pleno, los artículos 579 bis y 588 bis i no existían, pues fueron introducidos por Ley Orgánica 13/2015, de 5 de octubre.

Basta examinar ambos artículos de la Ley de Enjuiciamiento Criminal y el Acuerdo del Pleno para poner en duda que el Fiscal pueda "ordenar la transmisión de pruebas" en el derecho interno español. Es más, ni los artículos de la LECrim ni el Pleno hacen referencia siquiera al Ministerio Fiscal.

Principio del formulario

Final del formulario

El Tribunal Supremo se refiere después a otros tres preceptos de la Ley de Enjuiciamiento Criminal respecto de las facultades que el Fiscal tiene, como parte, para solicitar o aportar *motu proprio* información probatoria de un procedimiento a otro. Y así cita el art. 773.2 LECrim, que regula las denominadas Diligencias de Investigación que puede incoar el Ministerio Fiscal, y dos preceptos del Estatuto Orgánico del Ministerio Fiscal (arts. 5.2 y 4.3) haciéndose eco también de la Circular 2/2022 de 20 de diciembre de la Fiscalía General del Es-

tado. Pero, como en el caso anterior, el problema parece que no se termina de resolver de forma solvente.

La cuestión básica aquí es considerar si, como hace el Tribunal Supremo, la Orden Europea de Investigación cursada por el Ministerio Fiscal tenía por objeto simplemente la transmisión de información obtenida por las autoridades francesas o si, por el contrario, el hecho de que esa información fuera el fruto de la intervención de telecomunicaciones tiene algún tipo de relevancia.

Para el Tribunal Supremo no hay duda alguna: en la misma medida en que el Fiscal puede aportar antecedentes de intervenciones telefónicas de unas diligencias a otras, tampoco habría ningún problema en que pudiera recabar la información de Encrochat de las autoridades francesas.

El art. 187 de la Ley 23/2014 de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea reconoce que, efectivamente, los Fiscales son también autoridades de emisión en los procedimientos que dirijan, en nuestro caso, las Diligencias de Investigación. Pero sujetando dicha posibilidad a que la medida que contenga la orden europea de investigación no sea limitativa de derechos fundamentales además que la Fiscalía puede emitir órdenes europeas de investigación para la ejecución de medidas que podrían ordenar o ejecutar conforme a las disposiciones de la Ley de Enjuiciamiento Criminal.

En el caso que nos ocupa, el razonamiento del Tribunal Supremo parece insuficiente porque situar al mismo nivel una Orden Europea de Investigación cursada por la Fiscalía, por ejemplo, para aportar documentación de un registro público; con la Orden cursada por la Fiscalía para que le sea transmitida la información obtenida mediante la infección masiva con un virus informático de un sistema de comunicaciones de forma indiscriminada produce, cuando menos, insatisfacción. Una injerencia tan relevante reclama la intervención del juez, y no sólo la del Ministerio Fiscal.

5.2.- CONTROL A PRIORI DEL ESTADO DE EMISIÓN

El art. 6 de la Directiva 2014/41/CE del Parlamento y del Consejo de 3 de abril de 2014 relativa a la orden europea de investigación en materia penal prevé que la autoridad de emisión sólo puede llevar a cabo una Orden Europea de Investigación cuando se cumplan dos requisitos:

1. Cuando la emisión de la OEI sea necesaria y proporcionada a los fines de los procedimientos a que se refiere el artículo 4 teniendo en cuenta los derechos del sospechoso o acusado;
2. la medida o medidas de investigación requeridas en la OEI podrían haberse dictado en las mismas condiciones para un caso interno similar.

Por su parte, el artículo 189.1 de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, que traspone dicha Directiva, recoge los mismos requisitos, especificando en el segundo de ellos que la medida o medidas de investigación solicitadas cuyo reconocimiento y ejecución se pretende se hayan acordado en el proceso penal español en el que se emite la orden europea de investigación y pudieran haberse ordenado en las mismas condiciones para un caso interno similar.

El caso Encrochat supuso la emisión de una Orden Europea de Investigación dirigida no a que se practicara una concreta medida de investigación, sino para la transferencia de información en posesión de otro país como consecuencia de la investigación llevada a cabo por el mismo. De ahí que el Tribunal Supremo se plantee si estos dos requisitos cumulativos resultan de aplicación a dos casos distintos: órdenes de investigación sobre pruebas no practicadas y órdenes de investigación sobre pruebas ya practicadas.

Antes de que el TJUE dictara resolución sobre el caso concreto de Encrochat, las altas jurisdicciones de Alemania y Francia tomaron partido en el conflicto.

En el caso alemán, la Sentencia del Tribunal Supremo Federal de 02.03.2022 concluyó que la orden de investigación destinada a transmitir pruebas (no a practicarlas), la autoridad de emisión no tenía que examinar la medida de investigación porque la transferencia de pruebas ya practicadas no contiene una medida de investigación que se deba ejecutar.

En el caso italiano, la Sentencia de la Corte de Casación 6364/2023 de 15.01 parte desde otra perspectiva. Y así, entiende que se debe presumir que el Estado que ejecutó la medida de investigación lo hizo respetando la legalidad y los derechos fundamentales, salvo que en la práctica se pudiera verificar lo contrario.

El TJUE, por su parte, conocedor de estas soluciones de la jurisdicción alemana e italiana dictó Sentencia (Gran Sala) de 30.04.2024 en el asunto M.N. (C-670/22) que soluciona esta diatriba con una solución mixta entre las ya examinadas:

— De un lado, da carta de naturaleza a la existencia de dos tipos de órdenes: aquella que tiene por objeto la práctica de una prueba no ejecutado, y aquella que tiene por objeto la transmisión de datos en poder de una autoridad como consecuencia de haberse ejecutado previamente, conforme a su normativa interna, la correspondiente diligencia de investigación.

— Y así, situados en al orden de investigación "de transmisión de datos" el TJUE afirma que el art. 6.1 del Convenio debe aplicarse en el sentido de verificar si esa "transmisión de información" podría haberse llevado a cabo a nivel interno. O lo que es lo mismo: no cabe inmiscuirse en la diligencia de investigación llevada a cabo previamente, sino única y exclusivamente en el régimen de transmisión de información conforme al derecho interno.

— Pero, de otro, invoca el art. 82 TFUE para incidir en la confianza mutua que rige entre los Estados de la Unión en cuanto a que los mismos son respetuosos con los derechos fundamentales y las garantías procesales al uso, de donde se deduce que existe una presunción *iuris tantum* de que el estado emisor no ha solicitado esta orden de transmisión con la finalidad de eludir las propias normas internas.

En base a los criterios jurisprudenciales señalados previamente por parte del TJUE, el Tribunal Supremo español extraer cinco criterios generales:

1) El TJUE distingue entre OEI que se libran para la "recogida" de pruebas y las que se libran para la "transmisión" de pruebas. Esta distinción deriva de lo establecido en el art. 1, apartado 1, de la Directiva.

2) El control de una OEI para la "transmisión" de pruebas no exige un control a priori de los mismos requisitos de fondo aplicados, en el Estado de emisión, para la "recogida" de dichas pruebas.

3) Ello sigue siendo así, con independencia del lugar en que se hayan obtenido las pruebas, incluso si tal lugar es el propio territorio del Estado de emisión. Es indiferente si el Estado de ejecución de la OEI obtuvo las pruebas en su propio territorio, en el del Estado de emisión o en el de un tercer Estado. La solución es la misma, porque como indica el TJUE, la Directiva 2014/41, no varía el régimen aplicable a una OEI para la "transmisión" de pruebas, en función del lugar en el que se hayan recogido dichas pruebas.

4) El propio instrumento y las finalidades de la OEI y los principios del ordenamiento de la Unión Europea (especialmente, el de reconocimiento mutuo), implican una presunción iuris tantum de que los demás Estados miembros respetan el Derecho de la Unión y, en particular, los derechos fundamentales.

5) De todo lo dicho, se deriva que cuando la autoridad de emisión desee obtener la "transmisión" de pruebas en poder de otro Estado no está autorizada a controlar la regularidad del procedimiento mediante el que se hayan recogido las pruebas.

El Tribunal Supremo se esfuerza además en señalar que esta conclusión a la que llega, y estos criterios generales que extrae, no suponen una aceptación acrítica de los principios de no indagación, *locus regit actum* y *male captus bene detentus*. De hecho, afirma con rotundidad que la jurisprudencia de dicho alto tribunal ha matizado tales principios, entre otras, en las Sentencias del Tribunal Supremo 116/2017, 219/2021, 773/2021 y 1018/2021. Vale la pena traer a colación lo referido por la primera de dichas Sentencias, dictada en relación con los datos de la famosa Lista Falciani:

(…) que la prueba obtenida con vulneración de un derecho fundamental ha de ser excluida de la apreciación probatoria forma parte de las garantías del sistema constitucional. Más allá de su proclamación expresa en un enunciado normativo, su vigencia es nota definitoria del derecho a un proceso con todas las garantías. La exclusión de prueba ilícita del material valorable por el órgano decisorio forma parte del patrimonio jurídico de los sistemas democráticos. Y es que como proclamara esta Sala mediante un brocardo de obligada cita cuando se aborda esta materia, la verdad real no puede obtenerse a cualquier precio (cfr. ATS 18 de junio de 1992 –rec. 610/1990–). La necesidad de hacer eficaz esa regla de exclusión viene impuesta incluso por una exigencia ética ligada a la fuente legitimante de la función jurisdiccional. La incorporación de un acto lesivo de los derechos fundamentales al conjunto probatorio que ha de ser apreciado por el órgano sentenciador acarrea el riesgo de lo que la STS 195/2014, 3 de marzo, ha denominado una metástasis procesal. De ahí la importancia de que con anterioridad al proceso valorativo se proceda a un verdadero saneamiento del proceso, excluyendo aquellos elementos de prueba con virtualidad contaminante".

Y, más adelante en dicha Sentencia:

Es lógico que la validez en el proceso penal español de actos procesales practicados en el extranjero no se condicione al grado de similitud entre las reglas formales que, en uno y otro Estado, singularizan la práctica de esa prueba. Al juez español no le incumbe verificar un previo proceso de validación de la prueba practicada conforme a normas procesales extranjeras. Pero la histórica vigencia del principio locus regit actum, de dimensión conceptual renovada a raíz de la consolidación de un patrimonio jurídico europeo, no puede convertirse en un trasnochado adagio al servicio de la indiferencia de los órganos judiciales españoles frente a flagrantes vulneraciones de derechos fundamentales. Incluso en el plano semántico la expresión principio de no indagación, si se interpreta desbordando el ámbito exclusivamente formal que le es propio, resulta incompatible con algunos de los valores constitucionales comprometidos en el ejercicio de la función jurisdiccional". Y concluye después afirmando que "En definitiva, el principio de no indagación no puede interpretarse más allá de sus justos términos. Su invocación debería operar en el marco exclusivamente formal que afecta a la práctica de los actos de investigación en uno u otro espacio jurisdiccional. De tal forma que la flexibilidad admisible en los principios del procedimiento –adecuados por su propia naturaleza a cada sistema procesal– no se extienda a la obligada indagación de la vigencia de los principios estructurales del proceso, sin cuya realidad y constatación la tarea jurisdiccional se aparta de sus principios legitimadores.

Tanto el TJUE como el Tribunal supremo son conscientes de que la alineación de los estados de la Unión con los principios básicos y derechos fundamentales es una cuestión dinámica, y no estática. De ahí que el Tribunal Supremo valore como cautelas del TJUE que:

— La consideración de que la práctica de la prueba cuya información se traslada ha sido llevada a cabo cumpliendo los estándares europeos en materia de garantías procesales es una *presunción iuris tantum*.

— Y que, en cualquier caso, el recurso a una orden de investigación para la "transmisión de información" no tenga como objeto la elusión de las normas internas, lo que constituiría un claro caso de fraude de ley.

Sentado lo anterior, el Tribunal Supremo asume con facilidad la doctrina antes referenciada, y se limita a comprobar si, desde el punto de vista de la normativa española, es posible la transmisión de información, hallando su justificación en los ya citados arts. 579 bis y 588 bis i) LECrim, encontrando aquí su auténtico sentido.

Ciertamente, resulta sorprendente que el recurso a la normativa interna nos retrotrae nuevamente a un cierto control de la legalidad de la medida de investigación que da lugar a la información. En relación con el art. 588 bis i) LECrim se destaca que la admisibilidad de dicho traslado de información se vincula al control material de la legitimidad de la injerencia, lo que implica desechar la información obtenida con vulneración de derecho, dando lugar a la expulsión de dicha prueba conforme al art. 11 LOPJ.

Puesto que dicho control resulta necesario, el Tribunal Supremo lleva a cabo una notable pirueta jurídica y considera la legalidad de la medida de investigación ejecutada. Pero no lo hace

a la luz del derecho español (incompatible con lo que se ha referido hasta el momento), sino que la valora a la luz del derecho francés. De este modo no vulnera el principio de no indagación, pues no lleva a cabo un análisis de derecho comparado para revisar el ordenamiento jurídico francés a la luz del ordenamiento español. Sino que se limita a glosar cómo se llevó a cabo la medida de investigación en Francia y cuáles fueron las normas que amparaban su práctica.

Después de analizar, reiterativamente, el iter procesal seguido en Francia, el soporte indiciario existente en el país vecino y la normativa francesa aplicable concluye que la medida de investigación francesa es conforme a su derecho. Y no sólo eso, sino que considera que la misma no es una medida prospectiva y vulneradora de derechos fundamentales. Cuestión que no deja de ser paradójica si se han intervenido conversaciones de más de 38.000 usuarios.

Paradoja que resulta sorprendente cuando el Tribunal Supremo afirma que una injerencia masiva no es, necesariamente, prospectiva. Y ello en tanto que es conforme al derecho francés y porque existen indicios que justificarían la adopción de la medida. Hecho este reforzado por otros casos examinados por el TJUE (como el de Big Brother Watch), invocando conceptos escurridizos a la garantía procesal, tales como la existencia de amenazas a la seguridad nacional o contra los intereses nacionales esenciales.

Surgen preguntas inquietantes al hilo de la argumentación del Tribunal Supremo: ¿quién decide qué amenaza la seguridad nacional y cuáles son los intereses nacionales esenciales? Y, más relevante aún ¿cómo puede seguir llevando a cabo el poder judicial la función de salvaguarda de los derechos fundamentales de los ciudadanos si existen ámbitos que le vienen dados por el Estado (singularmente por el poder ejecutivo) que asume de forma acrítica porque no entra en su análisis?

5.3- CONTROL A POSTERIORI DEL ESTADO DE EMISIÓN

El Tribunal Supremo configura como control *a posteriori* la regulación de lo previsto en el art. 14 de la Directiva 2014/41/CE del Parlamento y del Consejo de 3 de abril de 2014 relativa a la orden europea de investigación en materia penal dedicada al recurso. Y más en concreto, a lo que se refiere en su artículo 14.7 cuando establece que los Estados miembros velarán por que, en los procesos penales en el Estado de emisión, se respeten los derechos de la defensa y la equidad del proceso al evaluar las pruebas obtenidas a través de la OEI.

Esta afirmación es definida como *críptica* porque parece que puede deducirse la posibilidad de que se examine la licitud de una medida ya ejecutada. Aunque finalmente salva esta aparente contradicción considerando que no existe tal control a posteriori de la autoridad de emisión, sino de una garantía añadida en el momento de utilizar y valorar la prueba en el procedimiento penal concreto, en función de la virtualidad de la información transferida pueda tener en el procedimiento en cuestión.

A este respecto, resulta interesante señalar que el Tribunal Supremo establece que los datos de Encrochat pueden desempeñar su función como:

— Medio de investigación.

— Medio de prueba.

— Indicio, en el contexto de prueba indiciaria.

— Medio de corroboración.

5.4.- LA NOTIFICACIÓN DEL ART. 31 DE LA DIRECTIVA: ¿DATO IRRELEVANTE?

La ya mencionada Directiva 2014/41/CE regula en el art. 31 el supuesto de una Orden Europea de Investigación destinada a la intervención de las telecomunicaciones suponga la utilización de dirección de comunicaciones de una persona que se encuentre en un estado distinto en el que un estado lleva a cabo una diligencia de investigación relativa a la intervención de las telecomunicaciones. Y para ello, se utilice la dirección de comunicaciones de personas que se encuentren fuera del estado que ejecuta la investigación. En estos casos, el mencionado art. 31 prevé que el estado que realiza la intervención notifique al Estado donde se encuentra esa persona la intervención de sus telecomunicaciones.

El supuesto abordado por el Tribunal Supremo parte de una premisa clara: en el caso Encrochat no existió notificación por parte de Francia a España en relación con la intervención de las telecomunicaciones a súbditos españoles residentes en este país. Y la cuestión que debe abordarse es qué efecto tiene esta ausencia de notificación y, lo que es más importante, cuál es su efecto procesal.

El Tribunal Supremo aborda esta cuestión deslindando primer cuál es el fin de esta notificación considerando que la misma es que el estado donde se encuentra el ciudadano intervenido pueda ejercer un control de dicha intervención. Control que, como refiere el art. 31.3 de la Directiva pasar por:

— El deber de valorar si la intervención se autorizaría en un caso similar conforme a la normativa nacional.

— En el caso de que considerase que no se autorizaría, tiene la facultad (podrá, dice la Directiva) de dirigirse al estado ejecutante para de la intervención para desautorizar la intervención, si aún no se ha llevado a cabo; o solicitar su cese, si estaba ya produciéndose.

— Y, en su caso, podrá también solicitar al estado ejecutante que no podrá utilizar como prueba el resultado de dicha intervención.

Para valorar esta autorización, el Tribunal Supremo centra sus esfuerzos argumentativos en el hecho de que la contestación del Estado notificado es de carácter potestativa. Más aún, cabe incluso el silencio como contestación.

En el caso Encrochat, es evidente que no se llevó a cabo la notificación correspondiente (Anexo C): no se solicitó la autorización ni antes ni durante ni tampoco después de realizada la intervención de las telecomunicaciones. Pero, a pesar de ello, el Tribunal Supremo entiende que la notificación del art. 31 no es un requisito sustancial que pueda afectar a la validez de la prueba. Y basa dicha insustancialidad en el hecho de que la notificación se puede remitir, precisamente, antes, durante o después de la intervención de las telecomunicaciones. Y se hace eco de la imaginativa interpretación que aporta el Ministerio Fiscal, conforme a la cual se parte de la evidencia de que no se ha remitido notificación. Pero el simple hecho de haber compartido de forma espontánea los datos obtenidos la interceptación es como si se hubiera llevado a cabo la notificación del art. 31 con posterioridad a la misma.

Esta interpretación del Fiscal, que el Tribunal Supremo hace suya y conduce a la irrelevancia de la notificación

contrasta poderosamente con el hecho de que en el Caso M.N., el TJUE refiere cómo el equipo conjunto de investigación instaba a las autoridades competentes de los Estados miembro a *confirmar por escrito* que habían sido informadas de los métodos empleados para recoger los datos procedentes de teléfonos móviles situados en el territorio nacional del Estado al que se le requería dicha confirmación escrita. Y también se debía garantizar que los datos transmitidos se usarían para su explotación, y sólo se utilizarían a los efectos de investigaciones en curso previa autorización de los Estados miembro del equipo conjunto de investigación. Si, como dicen el Fiscal y el Tribunal Supremo, la notificación es un requisito no esencial ¿por qué existen estas salvaguardias a las que se refiere el propio TJUE?

Finalmente, el Tribunal Supremo añade otro argumento para sostener la insustancialidad de la notificación de carácter material: es cierto que se interceptaron telecomunicaciones de nacionales españoles, pero la misma tuvo lugar directamente sobre un servidor situado en Francia. Y, por tanto, no existiría una medida transfronteriza que exija la aplicación del art. 31.

Es llamativo cómo ambos argumentos (la notificación no es requisito esencial vs. Inexistencia de injerencia transfronteriza) son en cierta medida incompatibles entre sí. Pues si gracias al virus informático se hubiera infectado un servidor situado en España ¿la autorización del art. 31 seguiría siendo insustancial?

Pero por su hubiera alguna duda, y los argumentos anteriores no resultaran convincentes, el Tribunal Supremo acude al ya clásico argumento de la efectiva indefensión: si faltó la notificación es la defensa la que tiene que demostrar que el incumplimiento de los requisitos previstos por la normativa comunitaria le generó indefensión. Inversión de la carga de la prueba que justifica por vía del art. 6.1 b) de la Directiva (ya examinado más arriba), debiendo presumirse salvo prueba en contrario que la actuación del estado miembro que autoriza la intervención de las telecomunicaciones es conforme con los derechos y garantías procesales del acervo comunitario.

5.5- CUERPO DE DOCTRINA DEL TRIBUNAL SUPREMO: CRITERIOS GENERALES

Finalmente cabe destacar la concreción de lo que podríamos denominar un cuerpo de doctrina del Tribunal Supremo en relación con el asunto Encrochat compuesto por criterios generales. Destacando las cuestiones procesales que pueden dar lugar los datos de Encrochat y que puede servir de prontuario a las defensas:

1. La forma de obtener los datos en Francia.
2. La técnica utilizada para obtener los datos, desconocida por tratarse de un secreto de defensa nacional en Francia.
3. La cadena de custodia de los datos.
4. La realización de copias.
5. La extracción de datos relativos a hechos, personas y delitos específicos.
6. La forma en que se lleva a cabo la incorporación de estos datos a cada procedimiento.

Y los informes policiales sobre la correspondencia entre Nick ñames e identidades.

Cabe destacar la sacralización de la doble criba o selección en cascada que sufren estos datos al llegar a España: la

selección hecha en Francia por las autoridades francesas, y una segunda criba sobre los anteriores realizada por las fuerzas policiales españolas. Sacralización que tiene como objetivo inocuizar el hecho de que jamás se ha puesto a disposición de las defensas los datos "en bruto" obtenidos por las autoridades francesas. Hecho este, evidentemente, lesivo del derecho de defensa ex art. 24 CE.

El Tribunal Supremo, con cita de otras Sentencias del TJUE (Caso Bylock, caso Big Brother Watch), aplica su propia doctrina general sobre el acceso de la defensa a la totalidad del material probatorio (entre otras, STS 993/2022 de 22.12 y 106/2023 de 16.02) que, en apretada síntesis, concluye que si a la defensa contó con medios y tiempo suficiente para preparar su defensa… el detalle de la falta de acceso a la totalidad de la información deviene, otra vez, un requisito no esencial.

Conclusiones

En lo que a cuestiones procesales se refiere podemos concluir:

1.- El Tribunal Supremo confiere carta de naturaleza al hecho de que el Ministerio Fiscal pueda cursar ordenes europeas de investigación con base en lo previsto en los arts. 579 bis, 588 bis i, ambos de la LECrim, y conforme con lo acordado en el Pleno No Jurisdiccional de 26.05.2009. Aunque ninguno de tales textos se refiere al Ministerio Fiscal y el hecho de que a fecha 26.05.2009 los preceptos referidos ni tan siquiera existiesen.

2.- No existe control a priori del Estado de emisión sobre el Estado de ejecución. Según el Tribunal Supremo, debe distinguirse entre órdenes europeas de investigación referidas a pruebas por practicarse y aquellas órdenes que se dirigen a transmitir datos de pruebas ya practicadas en el Estado de ejecución. Debe presumirse *iuris tantum* que la actuación del estado de ejecución fue conforme con los derechos fundamentales y garantías procesales, salvo prueba en contrario. Y debe verificarse, también, que la orden de investigación no tenía por finalidad la elusión de normas internas, dando lugar a un fraude de ley.

3.- No cabe tampoco un control a posteriori del Estado de emisión. Sí existe, por el contrario, una garantía añadida a la hora de utilizar y valorar esa prueba en el procedimiento penal en concreto.

4.- La falta de notificación ex art. 31 de la Directiva es un requisito insustancial para la determinación de la legalidad de la prueba obtenida a la luz del art. 11 LOPJ.

5.- Finalmente, el Tribunal Supremo sacraliza la falta de acceso de las defensas a los datos en bruto obtenidos por las autoridades francesas, dando carta de naturaleza al uso de datos que han sufrido una selección en cascada por parte, primero, de las autoridades francesas; y, después, por las autoridades policiales españolas.