Universidad Europea Madrid

LAUREATE INTERNATIONAL UNIVERSITIES

TRABAJO DE FIN DE GRADO

TÍTULO: "EL PAPEL DE EUROJUST EN LA LUCHA CONTRA EL CIBERCRIMEN TRANSFRONTERIZO EN LA UNIÓN EUROPEA: UN ANÁLISIS DE SU MARCO LEGAL Y SU EFICACIA EN LA COOPERACIÓN JUDICIAL"

AUTOR: ALEJANDRO GONZÁLEZ SERRÉ

TUTOR: Dr. JULIO GUINEA BONILLO

DOBLE GRADO EN DERECHO Y RELACIONES INTERNACIONALES

Curso académico 2022/2023

FACULTAD DE CIENCIAS SOCIALES Y DE LA COMUNICACIÓN

UNIVERSIDAD EUROPEA DE MADRID

“Europa no se hará de una vez ni en una obra de conjunto: se hará gracias a realizaciones concretas, que creen en primer lugar una solidaridad de hecho”.

-Robert Schuman

RESUMEN

El presente trabajo de investigación aborda el papel de Eurojust en la lucha contra el cibercrimen transfronterizo en la Unión Europea. Se realiza un análisis detallado de su marco legal y se evalúa su eficacia en términos de cooperación judicial. El objetivo es examinar cómo Eurojust contribuye al abordar los desafíos del cibercrimen en un contexto transnacional, considerando las herramientas legales y los mecanismos de cooperación que tiene a su disposición. Además, se busca determinar hasta qué punto Eurojust ha logrado cumplir su función en la lucha contra el cibercrimen, y qué mejoras podrían implementarse para fortalecer su eficacia en la cooperación judicial en este ámbito específico.

Palabras clave: Eurojust, ciberespacio, ciberseguridad, cibercrimen, cooperación judicial, Unión Europea.

ABSTRACT

This research project addresses the role of Eurojust in combating transnational cybercrime in the European Union. It provides a detailed analysis of Eurojust's legal framework and evaluates its effectiveness in terms of judicial cooperation. The objective is to examine how Eurojust contributes to tackling the challenges of cybercrime in a cross-border context, taking into account the legal tools and cooperation mechanisms at its disposal. Furthermore, the study aims to assess to what extent Eurojust has fulfilled its role in the fight against cybercrime and identifies potential improvements to enhance its effectiveness in judicial cooperation in this specific domain.

Keywords: Eurojust, cyberspace, cybersecurity, cybercrime, judicial cooperation, European Union.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE SIGLAS Y ABREVIATURAS

Sigla o abreviatura	Español	Inglés
API	Interfaz de Programación de Aplicaciones	Application Programming Interface
Art.	Artículo	Article
DDoS	Denegación de servicio distribuido	Distributed Denial of Service
EC3	Centro Europeo de Ciberdelincuencia	European Cybercrime Centre
ECIs	Equipos Conjuntos de Investigación	Joint Investigation Teams
ONUDD	Oficina de las Naciones Unidas contra la Droga y el Delito	United Nations Office on Drugs and Crime
RAE	Real Academia Española	Royal Spanish Academy
RJE	Red Judicial Europea	European Judicial Network
RSS	Sindicación Realmente Simple	Really Simple Syndication
TFUE	Tratado de Funcionamiento de la Unión Europea	Treaty on the Functioning of the European Union
TIC	Tecnologías de la Información y las Comunicaciones	Information and Communications Technology
TUE	Tratado de la Unión Europea	Treaty on European Union
UE	Unión Europea	European Union

ÍNDICE GENERAL

1. INTRODUCCIÓN

En la era digital actual, el cibercrimen transfronterizo se ha convertido en una amenaza significativa que trasciende las fronteras nacionales, y requiere una respuesta coordinada a nivel internacional. En este contexto, Eurojust, como agencia de cooperación judicial de la Unión Europea, desempeña un papel crucial en la lucha contra los delitos cibernéticos que afectan a múltiples países.

La expansión y la sofisticación del cibercrimen plantean desafíos significativos a los sistemas legales tradicionales, ya que los delincuentes aprovechan las ventajas del anonimato y la capacidad de operar a distancia. Teniendo en cuenta esto, Eurojust ha asumido un papel fundamental en la coordinación y cooperación entre las autoridades nacionales, y en la facilitación de investigaciones y procesos judiciales transfronterizos relacionados con el cibercrimen.

El presente estudio se enfocará en analizar el marco legal en el que Eurojust opera en el ámbito del cibercrimen transfronterizo, examinando las leyes y regulaciones existentes que respaldan sus acciones, y que promueven la cooperación jurídica internacional. Además, se evaluará la eficacia de Eurojust en la coordinación de investigaciones y en el fortalecimiento de la cooperación, entre las autoridades nacionales en la lucha contra el cibercrimen.

Los hallazgos de esta investigación serán de gran relevancia para comprender los desafíos legales y operativos que enfrenta Eurojust en su labor de combatir el cibercrimen transfronterizo en la Unión Europea. Asimismo, se espera que los resultados obtenidos contribuyan al debate académico y brinden recomendaciones para fortalecer el marco legal, y la eficacia de Eurojust en la cooperación jurídica internacional.

1.1. Objeto de la investigación

Investigación basada en el análisis exhaustivo del marco legal y la eficacia de Eurojust en la lucha contra el cibercrimen transfronterizo. A través de un enfoque detallado, se examinarán las políticas, regulaciones y prácticas operativas de Eurojust en relación con la ciberseguridad, centrándose en su capacidad para abordar los desafíos y las amenazas cibernéticas que trascienden las fronteras nacionales, y en la importancia de la cooperación judicial internacional.

1.2. Justificación

Se ha escogido esta temática por la creciente incidencia de delitos cibernéticos transfronterizos y la necesidad de una respuesta eficaz en el ámbito de las relaciones internacionales, que han puesto de manifiesto la importancia de abordar el papel de Eurojust en la lucha contra el cibercrimen. Es evidente que las formas de delitos cibernéticos están evolucionando rápidamente, y es crucial que los marcos legales y los mecanismos de cooperación internacional se mantengan actualizados, y sean efectivos para hacer frente a estos desafíos.

1.3. Objetivos

Los objetivos del presente trabajo son los siguientes:

- Objetivo general:

Analizar el marco legal, las funciones, las competencias, la eficacia y los nuevos retos de Eurojust en la lucha contra el cibercrimen transfronterizo, a través de la evaluación de su impacto en la cooperación judicial internacional, la identificación de deficiencias y desafíos, el nivel de especialización del marco legal de Eurojust y la exploración de nuevas tecnologías y enfoques innovadores, con el fin de proponer recomendaciones para fortalecer la capacidad de Eurojust como actor clave en la prevención y persecución del cibercrimen a nivel internacional.

- Objetivos específicos:

- Evaluar el marco legal actual de Eurojust en relación con el cibercrimen transfronterizo para determinar si proporciona o no el alcance, y los mecanismos de cooperación necesarios para hacer frente al cibercrimen transfronterizo.

- Investigar el alcance y los resultados de las actividades de cooperación judicial internacional de Eurojust en la lucha contra el crimen transfronterizo para determinar su impacto y eficacia.
- Comparar el nivel de especialización del marco legal de Eurojust y el enfoque del Convenio de Budapest en relación con el cibercrimen transnacional.
- Examinar en detalle las competencias y funciones de Eurojust relacionadas con la lucha contra el cibercrimen transfronterizo, evaluando su eficacia y capacidad para coordinar y apoyar las investigaciones, así como facilitar la cooperación entre los Estados miembros.
- Investigar y evaluar los nuevos retos, tecnologías y enfoques innovadores que pueden ser adoptados por Eurojust para mejorar la eficiencia y la eficacia de la cooperación jurídica internacional en la lucha contra el cibercrimen.
- Proponer recomendaciones y medidas concretas para fortalecer el papel de Eurojust, y promover sus funciones como actor clave en la lucha contra el crimen transfronterizo.

1.4. Hipótesis

1. El marco legal de Eurojust proporciona el alcance y los mecanismos de cooperación necesarios para hacer frente al cibercrimen transfronterizo.
2. El marco legal de Eurojust presenta un nivel de especialización insuficiente en la lucha contra el cibercrimen transnacional en comparación con el enfoque específico del Convenio de Budapest.
3. Eurojust cuenta con las funciones y competencias necesarias para hacer frente al cibercrimen transfronterizo.
4. Eurojust tiene un impacto limitado en la cooperación judicial internacional, y no ha logrado establecerse como un actor clave y eficaz en la lucha contra el cibercrimen transfronterizo.
5. La adopción de nuevas tecnologías y enfoques innovadores son necesarios para que Eurojust mejore la eficiencia y la eficacia de la cooperación jurídica internacional en los desafíos actuales y futuros.

1.5. Metodología

La metodología utilizada en el presente trabajo individual se basa en el método hipotético-deductivo, donde se busca obtener una conclusión que logre esclarecer la hipótesis planteada en el trabajo. Este enfoque conlleva la formulación de una hipótesis inicial, que es una suposición o afirmación tentativa sobre una relación o fenómeno. A partir de esta hipótesis, se deducen consecuencias lógicas y se plantean predicciones que pueden ser sometidas a pruebas empíricas.

Esto supone llevar a cabo un proceso sistemático de análisis, recolección y evaluación de evidencia relevante, con el objetivo de evaluar la validez y veracidad de las hipótesis. Se han utilizado diferentes técnicas y herramientas de investigación, como revisión de literatura, análisis de datos y estudio de casos, para obtener la información necesaria y desarrollar un argumento sólido.

En cuanto a la naturaleza de los datos, se ha seguido un enfoque cualitativo en este trabajo. Esto implica que se han buscado documentos e informes pertinentes relacionados con el tema de investigación. Estos datos cualitativos proporcionan una comprensión más profunda y detallada de los fenómenos, y permiten capturar la diversidad de perspectivas y experiencias. Se han utilizado técnicas como el análisis de contenido y la interpretación de datos para extraer información relevante y significativa.

La fuente principal utilizada en este trabajo es la investigación bibliográfica. Esto se traduce en la búsqueda exhaustiva de fuentes bibliográficas, como libros, artículos científicos, informes técnicos y documentos académicos, que sean relevantes para el tema de estudio. Se ha realizado una recopilación sistemática de información, organizándose de manera estructurada y evaluando críticamente su calidad y pertinencia. La investigación bibliográfica es fundamental para obtener una base sólida de conocimiento sobre el tema y respaldar el desarrollo de los argumentos y las conclusiones planteadas.

2. MARCO TEÓRICO-CONCEPTUAL

2.1. Definición de conceptos clave

2.1.1. Ciberespacio

Dentro de la comunidad de las Tecnologías de la Información y las Comunicaciones (TIC), el ciberespacio "refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos." (Fojón Chamorro & F. Sanz Villalba, 2010, p. 1).

Asimismo, puede definirse como “un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas” (Ottis & Lorents, 2010).

Otra definición dada que podemos encontrar es la siguiente: "el dominio global dentro del entorno de la información, que consiste en una infraestructura para la información tecnológica; lo que esencialmente, vienen a ser todas las máquinas conectadas a Internet y a la red que enlaza" (Newmeyer, 2015, p. 79).

Analizado lo anterior, podemos deducir que el ciberespacio está compuesto por diferentes elementos que interactúan entre sí. Estos elementos incluyen la infraestructura de red, que abarca tanto los componentes físicos como los lógicos, que permiten la interconexión de sistemas y dispositivos. También están presentes los sistemas y dispositivos, como ordenadores, teléfonos móviles y otros dispositivos electrónicos conectados a la red.

De igual modo, hay otros elementos que se pueden identificar como lo son los datos, que comprenden la información y los archivos almacenados y compartidos en línea. A su vez, los usuarios desempeñan un papel fundamental, ya que son las personas y las organizaciones que interactúan con el ciberespacio, accediendo, compartiendo y manipulando información.

Además, existen las aplicaciones y servicios en línea, como aplicaciones móviles, plataformas web y servicios en la nube, que operan en el ciberespacio y facilitan diversas funciones y actividades. Sin embargo, también hay amenazas y vulnerabilidades en el ciberespacio, como ataques cibernéticos y otros tipos de actividades maliciosas. Estas amenazas representan riesgos para la seguridad de los sistemas y la información en el ciberespacio.

Según María José Caro Bejarano (2011), aquellos que decidan operar en el ciberespacio, ya sean actores estatales o no, tendrán una serie de ventajas que a continuación se mencionan:

- "El ciberespacio es un «campo de batalla» de grandes dimensiones y donde resulta relativamente fácil asegurar el anonimato. Los ataques se pueden lanzar desde casi cualquier parte del mundo" (Bejarano, 2011, p. 52).
- Hay una desproporción entre el número de ataques y su coste, siendo este bastante reducido.
- Obliga a las víctimas a adoptar una actitud defensiva.
- Las amenazas tienen un alcance global.

Al analizar estas ventajas, se puede afirmar que el ciberespacio se asemeja a un extenso campo de batalla, donde las confrontaciones tienen lugar en un entorno virtual. Una de las características distintivas es la relativa facilidad para mantener el anonimato en este espacio digital. Los atacantes pueden lanzar sus ofensivas desde prácticamente cualquier ubicación geográfica, aprovechando la naturaleza global y conectada de Internet.

A menudo, los ataques cibernéticos son económicos. Esta circunstancia presenta un desafío significativo para las organizaciones y usuarios, ya que se ven obligados a asumir una actitud defensiva para proteger sus sistemas, redes y datos frente a las amenazas persistentes (Bejarano, 2011, p. 52).

Es importante resaltar que el alcance de las amenazas cibernéticas trasciende las fronteras nacionales, ya que el ciberespacio no está limitado por barreras geográficas (Bejarano, 2011, p. 52). Los ataques pueden afectar a múltiples regiones y países de manera simultánea. Esto enfatiza la necesidad de una colaboración internacional en la lucha contra las actividades maliciosas en línea, y la promoción de prácticas de ciberseguridad sólidas en todo el mundo.

2.1.2. Ciberseguridad

De entre todas las definiciones, una de las más aceptadas es la realizada por el doctor Kevin Newmeyer (2015) que define la ciberseguridad como "el conjunto de prácticas políticas, de entrenamiento y tecnología, diseñadas para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño" (Newmeyer, 2015, p. 79).

Por otro lado, una de las definiciones más recientes es la propuesta por Bermudez et al. (2023) que entiende la ciberseguridad como un término que "[...] abarca una amplia gama de prácticas, tecnologías y medidas diseñadas para proteger sistemas, redes y datos de ataques o accesos no autorizados. En la última década, los avances tecnológicos han permitido el desarrollo de técnicas de ciberseguridad más sofisticadas y robustas. Sin embargo, también han surgido nuevas y diversas formas de amenazas cibernéticas, obligando a la evolución constante del campo de la ciberseguridad." (Bermudez et al., 2023, p. 1).

Por su parte, Fojón et al. (2010) hace hincapié en que la definición de ciberseguridad ha ido cambiando a lo largo de los años. Inicialmente la ciberseguridad se centraba principalmente en proteger la información contra accesos no autorizados, usos indebidos, revelaciones no autorizadas, interrupciones, modificaciones o destrucciones no autorizadas (Fojón Chamorro & F. Sanz Villalba, 2010).

Sin embargo, en la actualidad, este enfoque ha evolucionado hacia la gestión de riesgos en el ciberespacio. Ahora, la ciberseguridad implica aplicar un proceso de

análisis y gestión de los riesgos asociados con el uso, procesamiento, almacenamiento y transmisión de información y datos, así como los sistemas y procesos utilizados. Todo esto se realiza siguiendo estándares internacionalmente aceptados (Fojón Chamorro & F. Sanz Villalba, 2010). Se puede entender que la ciberseguridad ha pasado de centrarse únicamente en proteger la información, a abordar de manera integral la gestión de riesgos en el ciberespacio.

La tecnología desempeña un papel fundamental en la ciberseguridad. Involucra el uso de herramientas y soluciones tecnológicas diseñadas para prevenir, detectar y responder a amenazas cibernéticas. Esto puede incluir *firewalls*[1], sistemas de detección y prevención de intrusiones, cifrado de datos, autenticación de dos factores y otros mecanismos de seguridad. Además, el diseño seguro de los dispositivos y sistemas es esencial para garantizar que operen según su diseño y no sean vulnerables a ataques (Bermudez et al., 2023).

También resulta relevante el entrenamiento en ciberseguridad, ya que este se refiere a la capacitación de individuos para desarrollar habilidades y conocimientos necesarios para proteger los sistemas informáticos. Este entrenamiento puede incluir la formación en técnicas de seguridad, identificación de amenazas, gestión de incidentes y mejores prácticas en el uso seguro de la tecnología (Newmeyer, 2015).

Sumado a lo anterior, las prácticas políticas en ciberseguridad implican establecer normas, regulaciones y directrices que promueven la seguridad de la información. Estas políticas pueden provenir de organismos gubernamentales, empresas o instituciones que buscan proteger sus sistemas y datos. Estas políticas pueden incluir requisitos de seguridad, protección de datos personales, medidas de cumplimiento y responsabilidad (Bermudez et al., 2023).

Por lo tanto, de todas estas definiciones presentadas, podemos inferir que la ciberseguridad abarca aquellas prácticas y políticas en ciberseguridad que implican

[1] La palabra *firewalls* se refiere a lo conocido como “cortafuegos” definido por la Real Academia Española (RAE) como: “sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet.”.

establecer normas, regulaciones y directrices que promueven la seguridad de la información.

En definitiva, el conjunto de prácticas políticas, entrenamiento y tecnología en ciberseguridad tiene como objetivo proteger el entorno cibernético, preservar la integridad de la información y asegurar la capacidad de conectar dispositivos para que operen de manera segura y confiable. Esto implica establecer políticas de seguridad, capacitar a las personas en ciberseguridad y utilizar tecnologías adecuadas para prevenir y responder a las amenazas cibernéticas.

2.1.3. Cibercrimen

El cibercrimen o ciberdelito[2] está definido como "cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito" (Rayón Ballesteros & Gómez Hernández, 2014, p. 211).

Resulta aparente que abordar este tipo de criminalidad requiere adoptar un enfoque a nivel supranacional, mediante la creación de unidades de investigación policial especializadas y equipadas con los recursos técnicos necesarios, para llevar a cabo su labor de manera eficaz. Asimismo, es necesario establecer procedimientos judiciales ágiles y especializados para tratar este tipo de comportamientos delictivos (Rayón Ballesteros & Gómez Hernández, 2014).

Otra definición para cibercrimen es la que se refiere a crímenes realizados usando Internet u otro tipo de redes propias de los ordenadores, que son utilizados para cometer este tipo de crímenes. Esto es debido principalmente a que el ordenador o

[2] Al no ser una cuestión principal sobre la que versa el presente trabajo, pero no por ello menos relevante, cabe mencionar que en la publicación del Anuario jurídico y económico escurialense, Rayón Ballesteros & Gómez Hernández realizan una aclaración sobre la diferencia entre delito informático y el ciberdelito, cuestión para la cual se recomienda la consulta de Romeo Casabona, Carlos. “De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal” en El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales. Editorial Comares. Granada 2006, pp. 1-42.

la red puede ser el arma o el objetivo para cometer el crimen, o puede ser usada para propósitos incidentales relacionados al crimen (Valdez Alvarado, 2012).

Valdez (2012), realiza una clasificación de los distintos tipos de cibercrimen en función de si existe violencia o no. La clasificación es la siguiente:

- Cibercrímenes violentos o potencialmente violentos: ciberterrorismo, amenazas de ataques, ciberespionaje y pornografía infantil.
- Cibercrímenes no violentos: ciberviolaciones, ciberrobo, ciberfraude, apuestas por internet, venta de drogas por Internet, blanqueo de dinero, cibercontrabando y la publicidad o solicitud de prostitución en Internet.

A día de hoy siguen surgiendo nuevas técnicas y modalidades de cibercrimen como *phishing*[3], *skimming*[4], o los numerosos intentos de introducir programas maliciosos en los dispositivos tecnológicos con acceso a Internet (Prado, 2022).

Recapitulando, entendemos por cibercrimen al conjunto de actividades delictivas que se llevan a cabo a través de medios electrónicos o digitales, utilizando tecnologías de la información y las comunicaciones. Estas actividades criminales pueden incluir el acceso no autorizado a sistemas informáticos, el robo de información confidencial, el fraude en línea, el sabotaje de redes, el *phishing*, los programas maliciosos y el ciberacoso entre otros.

2.1.4. Cooperación judicial internacional

La cooperación judicial internacional se ha basado tradicionalmente en la necesidad de prevenir y combatir los delitos y fraudes, que surgen como consecuencia de las interacciones sociales y económicas entre diferentes grupos y organizaciones ubicadas en distintos países. Estas interacciones se desarrollan en un contexto de soberanía legislativa y judicial, con leyes y jurisdicciones claramente definidas. En

[3] El *phishing* es una técnica que consiste en enviar correos electrónicos fraudulentos a los usuarios, haciéndose pasar por una organización legítima, con el fin de engañar a las personas para que revelen información confidencial como contraseñas o números de tarjetas.
[4] El *skimming* consiste en la clonación de tarjetas de crédito.

este sentido, la cooperación internacional busca garantizar la responsabilidad y evitar la impunidad de aquellos que cometen o participan en estos hechos criminales y fraudulentos (Abreu Valencia, 2022).

El enfoque tradicional de cooperación internacional se caracteriza por la identificación clara y precisa de los elementos relacionados con los hechos o actos delictivos. Estos elementos suelen estar debidamente identificados, ya sea a través de evidencias tangibles como armas, huellas dactilares o documentos físicos, o mediante testimonios y declaraciones que proporcionan información detallada sobre los acontecimientos en cuestión. Esta capacidad de identificación precisa, ha sido históricamente importante para determinar con certeza el lugar exacto donde se produjeron los hechos delictivos, así como para establecer la identidad y la nacionalidad, o residencia de los individuos responsables de su perpetración (Abreu Valencia, 2022).

Según Abreu Valencia (2022) esta identificación precisa se basa en la disponibilidad de pruebas concretas y testimonios verificables, lo que ha permitido una mayor eficacia en la investigación y enjuiciamiento de los delitos a nivel internacional. Además, la existencia de documentos físicos y otros tipos de evidencia tangible han facilitado el proceso de recopilación de pruebas y su presentación en los tribunales. De igual modo, la obtención de testimonios y declaraciones testimoniales ha contribuido a esclarecer los hechos y proporcionar información valiosa para la identificación y persecución de los responsables.

Sin embargo, es importante tener en cuenta que el avance de las tecnologías digitales y el crecimiento de los delitos cibernéticos han planteado nuevos desafíos para este enfoque tradicional de cooperación judicial internacional. En estos casos, la identificación de los responsables puede resultar más compleja debido a la naturaleza virtual y globalizada de los delitos cibernéticos, así como a la capacidad de los ciberdelincuentes para ocultar su identidad y ubicación. Por lo tanto, se requieren enfoques y estrategias actualizadas, para abordar eficazmente estos

nuevos desafíos en el ámbito de la cooperación jurídica internacional (Abreu Valencia, 2022).

La cooperación internacional se ha convertido en una necesidad imperante en nuestro mundo globalizado. En un entorno cada vez más interconectado, es esencial que los países trabajen juntos para abordar desafíos comunes, como el cambio climático, el terrorismo, la migración y la pandemia de enfermedades (Abreu Valencia, 2022).

Esta cooperación se manifiesta a través de un conjunto de normas y regulaciones establecidas en acuerdos y tratados internacionales. Estas normas actúan como un marco que guía las relaciones entre los Estados, facilitando la colaboración y promoviendo la estabilidad y el desarrollo sostenible. Dentro del ámbito legal nacional, se busca facilitar la asistencia entre países de manera discrecional. Esto significa que las autoridades nacionales tienen la flexibilidad de brindar apoyo y cooperación según las circunstancias y los principios de cortesía internacional. En otras palabras, se busca promover una actitud de reciprocidad[5] y buena voluntad en las relaciones bilaterales y multilaterales (Abreu Valencia, 2022).

2.1.5. Eurojust

La idea de establecer un espacio judicial europeo en materia penal, que incluiría diversas etapas, fue planteada por Giscard d'Estaing en 1977, contemplando diversas fases progresivas. Entre ellas se encontraban la elaboración de un tratado de extradición simplificado, la mejora y flexibilización del mecanismo de asistencia judicial, el reconocimiento de la ejecución de sentencias y la generalización del traslado de reclusos entre centros penitenciarios, entre otros aspectos. No obstante, sólo décadas después se comenzaron a rescatar algunas de las ideas originales francesas, y la noción de una Unidad de Cooperación Judicial como Eurojust

[5] En el compendio publicado por la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), comúnmente conocido por sus siglas en inglés “UNODC”, se menciona que los criterios de reciprocidad desempeñan un papel crucial en este proceso. Cuando un país ofrece ayuda o cooperación a otro, se espera que haya una respuesta recíproca por parte del país beneficiado, fortaleciendo la confianza mutua.

empezó a cobrar sentido, con el propósito de superar los habituales obstáculos en la cooperación jurídica internacional (Pérez Souto, 2013).

Con el propósito de adquirir un entendimiento completo, es preciso remontarnos al Tratado de Maastricht firmado el 7 de febrero de 1992 y cuya entrada en vigor fue el 1 de noviembre de 1993. En su origen, dicho tratado consideraba la cooperación judicial como un asunto de interés común. No obstante, en la práctica se hizo evidente que la cooperación se encontraba en una situación caracterizada por la falta de definición de objetivos, y la ausencia de mecanismos institucionales que unificase un espacio común de seguridad y justicia. Además, se presentaba un desafío adicional: los Estados miembros defendían constantemente sus diferencias culturales en cuanto a la concepción de la justicia, particularmente en lo referente a la legislación penal. Esta diversidad de enfoques resultaba poco compatible con el necesario sentimiento de confianza mutua que debe prevalecer en cualquier proceso de integración. Así pues, se requería una solución que superara los obstáculos y permitiera una cooperación más eficaz en el ámbito judicial para combatir el crimen transnacional grave (Pérez Souto, 2013).

Este impulso se materializaba en el Consejo Europeo de Tampere, convocado los días 15 y 16 de octubre de 1999, con el propósito de promover de manera realista el Espacio de Libertad, Seguridad y Justicia. Eurojust emergió como el principal instrumento de cooperación y ocupó un lugar destacado en la agenda política. El Consejo Europeo estableció orientaciones y objetivos concretos, respaldados por un calendario, con el objetivo de prevenir que la delincuencia organizada transnacional se aprovechara de las diferencias existentes entre los sistemas judiciales de los Estados miembros (Pérez Souto, 2013).

Así queda reflejado en la siguiente cita: "Las conclusiones de Tampere conducían a la necesidad práctica de que las sentencias y resoluciones debían respetarse y ejecutarse en toda la Unión, salvaguardando al mismo tiempo la seguridad jurídica y logrando que aumentase la compatibilidad y la convergencia de los sistemas judiciales de los Estados miembros" (Pérez Souto, 2013, p. 4).

Por su parte, el Tratado de Ámsterdam, firmado en 1997 y en vigor a partir de 1999, fue un hito importante en la evolución de la Unión Europea. Este tratado introdujo importantes cambios institucionales y jurídicos para fortalecer la cooperación en materia de justicia y asuntos internos (Pérez Souto, 2013).

El respaldo definitivo a la creación de Eurojust tuvo lugar en el año 2002 tras un acontecimiento de gran impacto: los atentados terroristas del 11 de septiembre de 2001 en Estados Unidos. Estos trágicos sucesos desempeñaron un papel determinante en la decisión de establecer Eurojust para poder responder de manera rápida y eficaz a los delitos de carácter transnacional como podría ser la lucha contra el terrorismo. Se creó así Eurojust, a través de la Decisión 2002/187/JAI del Consejo como una entidad con personalidad jurídica dentro de la Unión Europea. Su principal objetivo era promover y mejorar la coordinación y cooperación entre las autoridades judiciales competentes de los Estados miembros, especialmente en casos de delincuencia organizada grave (Pérez Souto, 2013).

Tras dos décadas de funcionamiento, Eurojust ha logrado consolidarse como una institución sólida, respaldando el compromiso constante de la Unión Europea en la construcción de un espacio real de libertad, seguridad y justicia en su territorio. En este sentido, Eurojust desempeña un papel vital al fomentar una mayor integración en el ámbito de la cooperación judicial penal entre los Estados miembros (Torres Pérez, 2022).

En definitiva, la labor de Eurojust se extiende más allá de la mera cooperación jurídica, ya que también contribuye a fortalecer la confianza mutua entre los Estados miembros. La existencia de una entidad como Eurojust, capaz de abordar los desafíos transfronterizos en la lucha contra el crimen grave, fomenta la solidaridad y el entendimiento entre los países europeos, sentando las bases para una colaboración más estrecha y una respuesta más eficiente frente a las amenazas transnacionales.

2.2. Revisión de literatura académica

Los criterios utilizados en la revisión de la literatura académica son los siguientes:

En primer lugar, por su relevancia temática. Se han seleccionado fuentes que están directamente relacionadas con el papel de Eurojust en la lucha contra el ciberdelito transfronterizo en la Unión Europea. Esto ha implicado buscar estudios, informes, artículos académicos y libros que abordan específicamente este tema.

En segundo lugar, en base a criterios de autoridad, credibilidad y rigor académico. Por ello, se ha optado por fuentes escritas por académicos, expertos en el campo del derecho internacional, ciberseguridad, cooperación judicial o áreas relacionadas, así como fuentes provenientes de instituciones reconocidas, revistas científicas y editoriales académicas.

En tercer lugar, de acuerdo a un criterio de actualidad. El ciberdelito y las políticas de cooperación judicial están en constante evolución. Por lo tanto, es fundamental seleccionar fuentes actualizadas y que reflejen los desarrollos más recientes en el marco legal, y las estrategias de Eurojust en relación con el ciberdelito transfronterizo.

En cuarto y último lugar, por sus perspectivas diversas. Se han buscado fuentes que presenten diferentes perspectivas y enfoques en relación con el tema. Esto permitirá obtener una visión más completa y equilibrada de la eficacia de Eurojust en la lucha contra el ciberdelito transfronterizo en la Unión Europea.

2.2.1. Estudios e investigaciones sobre cibercrimen transfronterizo y sus implicaciones

- Abreu Valencia, F. A. (2022): este autor ha investigado específicamente la cooperación internacional en materia de cibercrimen y evidencia digital. Su artículo en la revista "Saber y Justicia" aborda de manera detallada las implicaciones de la cooperación internacional en la lucha contra el

cibercrimen. Su enfoque en la evidencia digital es especialmente relevante para comprender los desafíos y las soluciones en este campo.

- Bejarano, M. J. C. (2011): este autor, en su trabajo para el Instituto Español de Estudios Estratégicos, se enfoca en el alcance y el ámbito de la seguridad nacional en el ciberespacio. Su investigación ofrece una perspectiva específica sobre la importancia de la seguridad en el ciberespacio, y cómo esto se relaciona con el cibercrimen transfronterizo.

- Díaz Gómez, A. (2010): el autor analiza el delito informático y su problemática, centrándose en el papel de la cooperación internacional, especialmente a través del Convenio de Budapest.

- Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014): estos autores han abordado las particularidades en la investigación y enjuiciamiento del cibercrimen. Su artículo en el Anuario jurídico y económico escurialense proporciona información detallada sobre los desafíos y enfoques necesarios en la lucha contra el cibercrimen.

2.2.2. Estudios e investigaciones sobre el papel de Eurojust en la cooperación judicial internacional

- Alonso Moreda, N. (2012): este autor ha investigado específicamente el papel de Eurojust en la cooperación judicial en materia penal en la Unión Europea. Su artículo en la "Revista de Derecho Comunitario Europeo" analiza a fondo las funciones y el impacto de Eurojust en la lucha contra el crimen transfronterizo en el ámbito penal. Su enfoque en la vanguardia de la cooperación judicial y su análisis detallado del marco legal y las actividades de Eurojust, hacen de este recurso una fuente de autoridad y credibilidad para comprender el papel y la eficacia de Eurojust en la cooperación judicial en la Unión Europea.

- Brière, C. (2018): en su artículo se examina la cooperación de Europol y Eurojust con socios externos en la lucha contra el crimen. Su enfoque en los desafíos que enfrentan estas agencias es relevante para comprender el contexto en el que Eurojust opera, y en cómo interactúa con otras organizaciones en la lucha contra el cibercrimen transfronterizo.

- Escalada López, M. L. (2023): el autor examina en detalle la cooperación judicial en la Unión Europea, centrándose específicamente en Eurojust y las novedades normativas que le conciernen. El artículo proporciona un análisis exhaustivo de la evolución de Eurojust y las implicaciones de las nuevas regulaciones para su funcionamiento y eficacia en la cooperación judicial transfronteriza.

- Hernández López, A. (2020): el autor examina las fortalezas y debilidades del Reglamento de Eurojust, en particular su relación con los artículos 85 y 86 del Tratado de Funcionamiento de la Unión Europea (TFUE). El estudio proporciona una evaluación crítica de los aspectos legales y operativos de Eurojust, lo cual resulta relevante para comprender su marco legal, funciones y competencias.

- Pérez Souto, G. (2013): el autor ha investigado sobre Eurojust y su eficacia en la lucha contra el crimen organizado. Su artículo en la Revista General de Derecho Europeo ofrece una evaluación crítica y reflexiva sobre el papel de Eurojust.

- Torres Pérez, M. (2022): el autor se ha centrado en Eurojust y su papel en la cooperación judicial penal en Europa. Su trabajo reciente sobre el futuro de Eurojust en el contexto de la guerra en Ucrania ofrece una perspectiva actualizada y pertinente sobre el tema.

2.3. Marco legal e institucional

2.3.1. Tratados y acuerdos internacionales relevantes en la cooperación judicial internacional

A continuación se presentan los tratados y acuerdos internacionales[6] más relevantes que guardan alguna relación de acuerdo con el objeto del presente trabajo en el ámbito de la cooperación judicial internacional:

- Resolución aprobada por la Asamblea General 55/25. Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, (2000) también conocida como la Convención de Palermo.

En la parte principal de la citada Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional se encuentran las medidas de prevención y lucha contra la delincuencia organizada transnacional, las medidas relativas a la cooperación internacional y el mecanismo de revisión de la aplicación de la Convención. Estas secciones establecen disposiciones generales para prevenir y combatir la delincuencia organizada, incluyendo medidas para fortalecer las leyes y regulaciones nacionales, así como para promover la cooperación y el intercambio de información entre los Estados miembros.

En la segunda parte se incluyen una serie de protocolos. El primer protocolo hace referencia a cuestiones para prevenir, reprimir y sancionar la trata de personas, especialmente de mujeres y niños. El segundo protocolo se centra en el tráfico ilícito de migrantes por tierra, mar y aire. Por último hay un protocolo anexo contra la

[6] Resulta importante señalar que los dos primeros tratados y acuerdos internacionales mencionados en este apartado (Resolución 55/25 y Resolución 58/4 de la Asamblea General) no fueron elaborados con el objetivo principal de abordar el cibercrimen, si bien pueden servir para fundamentar o complementar algunas disposiciones de aquellos creados de manera específica y concreta para prevenir, combatir y sancionar el cibercrimen internacional. Sumado a lo anterior, hay otros ejemplos que se pueden mencionar como la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes de 1987 o la Convención de La Haya sobre los Aspectos Civiles de la Sustracción Internacional de Menores de 1980 entre otros, entendiendo que estos últimos no guardan relación alguna con el tema del presente trabajo.

fabricación y tráfico Ilícitos de armas de fuego, sus piezas, componentes y municiones.

- Resolución 58/4 de la Asamblea General, de 31 de octubre de 2003. Convención de las Naciones Unidas contra la Corrupción.

Su objetivo principal es prevenir y combatir la corrupción a nivel nacional e internacional, así como promover la integridad, la transparencia y la rendición de cuentas en el sector público y privado.

En primer lugar, se insta a los Estados miembros a tomar medidas para prevenir la corrupción en el sector público, promoviendo la transparencia, la participación ciudadana, la ética y la educación anticorrupción. En segundo lugar, se señalan las medidas penales y aplicación de la ley, estableciendo disposiciones para tipificar como delitos una amplia gama de actos de corrupción, como el soborno, el enriquecimiento ilícito, el tráfico de influencias y el blanqueo de dinero. La recuperación de activos también es una parte importante, estableciendo así medidas para facilitar la identificación, incautación y devolución de activos obtenidos a través de actos de corrupción.

También se remarca la importancia en la cooperación internacional, al fomentar la cooperación entre los Estados en la prevención y lucha contra la corrupción, y creando mecanismos para el intercambio de información, la asistencia legal mutua, la extradición y la transferencia de condenados.

- Convenio de Budapest sobre la ciberdelincuencia del 23 de noviembre de 2001.

Aunque no es una normativa de la Unión Europea, el Convenio de Budapest es un tratado internacional que ha sido ratificado por varios países europeos y establece un marco legal para la cooperación transfronteriza en la lucha contra el cibercrimen.

Es importante destacar que el Convenio de Budapest no solo involucra a los países del Consejo de Europa, sino que también está abierto a la adhesión de Estados no miembros. Además, el convenio ha sido complementado por protocolos adicionales que tratan aspectos específicos de la ciberdelincuencia, como la trata de seres humanos y la falsificación de moneda.

2.3.2. Legislación y tratados de la Unión Europea en materia de cibercrimen y cooperación transfronteriza

A continuación se presenta la legislación, tratados y reglamentos de la Unión Europea (UE) de mayor relevancia en materia de cibercrimen y cooperación transfronteriza:

- Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011 , relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

- Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 , relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»).

2.3.3. Regulación de Eurojust: Reglamento sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust)

El reglamento que actualmente se encuentra en vigor y dota a Eurojust de personalidad jurídica es el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo.

El citado reglamento se compone de varios capítulos siendo estos:

Capítulo I. El reglamento define el objeto, las funciones de Eurojust y las competencias en las que se incluyen facilitar y mejorar la cooperación judicial y la coordinación de investigaciones y enjuiciamientos en asuntos penales transfronterizos. Eurojust tiene como objetivo principal fomentar la cooperación entre las autoridades nacionales encargadas de hacer cumplir la ley de los Estados miembros.

Capítulo II. Se establece la estructura y organización de Eurojust, incluyendo su composición, órganos de toma de decisiones y designación de sus miembros. También establece las normas de funcionamiento, el mandato de los miembros y las disposiciones sobre la confidencialidad y protección de datos.

Capítulo III, IV y V. Se establecen las cuestiones operativas como la cooperación con otras instituciones y organismos, y las relaciones entre los socios. El reglamento prevé la cooperación de Eurojust con otras instituciones y organismos de la UE, como Europol y la Agencia de Derechos Fundamentales de la Unión Europea.

Establece mecanismos de intercambio de información y coordinación para promover una cooperación eficiente en la lucha contra la delincuencia transfronteriza.

Capítulo VI, VII y VIII. Se establecen las disposiciones financieras y de personal, así como la elaboración y ejecución del presupuesto, rendición de cuentas, aprobación de la gestión y la evaluación y elaboración de informes. También permite a Eurojust contar con la asistencia de expertos nacionales ajenos a Eurojust.

Capítulo IX. Contiene las disposiciones finales tales como los privilegios e inmunidades, el régimen lingüístico, confidencialidad y diversas normas sobre la protección de la información sensible no clasificada y clasificada intercambiada entre Eurojust y las autoridades nacionales. Estas disposiciones garantizan el tratamiento adecuado de los datos personales y la confidencialidad de la información sensible.

3. DESARROLLO DE LA INVESTIGACIÓN

3.1. Estudio de los marcos legales

3.1.1. Análisis de las normativas que sustentan la actuación de Eurojust en la lucha contra el cibercrimen transfronterizo

El Reglamento (UE) 2018/1727 sobre Eurojust es la norma principal que establece los objetivos y alcance de la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust), reemplazando y derogando la Decisión 2002/187/JAI del Consejo. En el citado reglamento, se establece que el principal objetivo de Eurojust es fortalecer la cooperación judicial penal entre los Estados miembros de la Unión Europea en la lucha contra la delincuencia grave y transfronteriza. Se busca facilitar el intercambio de información, la coordinación de investigaciones y la asistencia mutua entre las autoridades nacionales competentes. A este reglamento, en función del objeto en cuestión podrán resultar de aplicación los diferentes tratados o acuerdos de índole internacional, así como la legislación europea.

3.1.1.1. Alcance de las normativas

El alcance de las normativas que sustentan la actuación de Eurojust en la lucha contra el crimen transfronterizo es un aspecto fundamental para comprender la eficacia y el impacto de dichas normativas en la protección de la ciberseguridad. Estas normativas están diseñadas para abordar los delitos cibernéticos y promover la cooperación judicial penal entre los Estados miembros de la Unión Europea (Newmeyer, 2015).

Es importante destacar que las normativas abarcan una amplia gama de delitos que afectan a la ciberseguridad, incluyendo el acceso no autorizado a sistemas informáticos, el fraude electrónico, el robo de datos, la difusión de virus informáticos y la pornografía infantil en línea entre otros. Estos delitos representan una amenaza significativa para la ciberseguridad y la privacidad de los ciudadanos, así como para el funcionamiento de las instituciones y las empresas.

En este sentido, las normativas buscan establecer un marco legal y operativo que permita a Eurojust y otras autoridades competentes cooperar de manera eficaz en la lucha contra el cibercrimen transfronterizo. Esto implica la promoción de la cooperación transfronteriza en la obtención y el intercambio de información y pruebas digitales, así como la armonización de los marcos legales y los procedimientos de investigación entre los Estados miembros (Pérez Souto, 2013).

El alcance de estas normativas también abarca a la prevención y disuasión del cibercrimen. Se busca establecer medidas y mecanismos que desalienten la comisión de delitos cibernéticos, mediante la creación de un marco legal claro y disuasorio, así como la promoción de la concienciación y la educación en materia de la ciberseguridad (Newmeyer, 2015).

Además, las normativas tienen como objetivo principal la identificación y persecución de los delincuentes cibernéticos. Esto implica la cooperación estrecha entre las autoridades judiciales y fiscales de los Estados miembros, así como el uso de

herramientas y técnicas especializadas para investigar y enjuiciar los delitos cibernéticos. Las normativas también buscan garantizar la protección de las víctimas de cibercrimen y promover su acceso a la justicia (Pérez Souto, 2013).

3.1.1.2. Mecanismos de cooperación

Estas normativas contemplan la designación de puntos de contacto especializados en cibercrimen en cada Estado miembro. Estos puntos de contacto son responsables de facilitar la comunicación y la coordinación entre las autoridades competentes en casos de delitos cibernéticos. Su papel es fundamental para agilizar los procesos de intercambio de información, solicitudes de asistencia y coordinación de acciones conjuntas.

La normativa, en concreto el Reglamento (UE) 2018/1727 sobre Eurojust establece procedimientos claros para el intercambio de información relevante entre las autoridades judiciales y fiscales de los Estados miembros tal y como queda reflejado en el artículo 21.1[7] y 21.3[8] de dicho reglamento. Esto incluye tanto el intercambio de datos personales como el de evidencias digitales. Los mecanismos de cooperación aseguran que esta información sea compartida de manera rápida y segura, preservando la confidencialidad y garantizando la integridad de los datos.

Asimismo, las normativas promueven la coordinación de investigaciones y la realización de operaciones conjuntas. Esto queda reflejado en el artículo 21.4 del reglamento con la creación de los denominados “Equipos Conjuntos de Investigación” (ECIs). Esto implica que las autoridades competentes de diferentes países trabajen en estrecha colaboración para identificar y desmantelar redes delictivas que operan en el ámbito cibernético. Estas operaciones conjuntas

[7] Artículo 21.1 del Reglamento (UE) 2018/1727 sobre Eurojust: “Las autoridades competentes de los Estados miembros intercambiarán con Eurojust toda información necesaria con miras al cumplimiento de las funciones de esta última en virtud de lo dispuesto en los artículos 2 y 4, y de conformidad con las normas aplicables en materia de protección de datos. Esto incluirá como mínimo la información a que se refieren los apartados 4, 5 y 6 del presente artículo.”.

[8] Artículo 21.3 del Reglamento (UE) 2018/1727 sobre Eurojust: “Los miembros nacionales intercambiarán, sin previa autorización, entre sí o con las autoridades nacionales competentes, toda información necesaria para el cumplimiento de las funciones de Eurojust. En particular, las autoridades nacionales competentes informarán sin demora a sus miembros nacionales de todo caso que les afecte.”.

permiten una respuesta más eficaz y contundente contra el cibercrimen, al unir recursos, conocimientos y experiencia de múltiples jurisdicciones (Alonso Moreda, 2012).

Según Alonso Moreda (2012) la formación de los ECIs es una valiosa herramienta de colaboración en la lucha contra la delincuencia transfronteriza. Estos equipos reúnen a investigadores, fiscales y jueces en un mismo espacio de trabajo, lo que facilita la recopilación de pruebas dentro de un marco legal establecido. La participación de Eurojust en la capacitación y en las actividades de los ECIs ayuda a mejorar su eficacia en esta tarea.

La participación de Eurojust en los ECIs se caracteriza por su enfoque integral y multidimensional para fortalecer la cooperación transfronteriza en la lucha contra la delincuencia. Además de brindar asesoramiento específico y coordinación, Eurojust desempeña un papel crucial en el respaldo operativo de los ECIs (Alonso Moreda, 2012).

Este respaldo operativo se materializa en diversas formas, como proporcionar recursos técnicos y financieros para respaldar las investigaciones conjuntas, facilitar el intercambio rápido de información y evidencia entre los equipos, y coordinar estrechamente con otras agencias y organismos competentes. Además, Eurojust se involucra activamente en la promoción de la estandarización de los procedimientos y la armonización de las normas legales en los países participantes, lo que permite una mayor eficiencia y eficacia en el trabajo de los ECIs (Alonso Moreda, 2012).

En conjunto, la participación de Eurojust en los ECIs abarca desde el asesoramiento hasta el respaldo operativo, la promoción de estándares y la divulgación de buenas prácticas. Estas acciones combinadas tienen como objetivo mejorar la eficacia y eficiencia de los ECIs, fortaleciendo así la capacidad de respuesta ante la delincuencia transfronteriza y fomentando una cooperación más estrecha entre los actores involucrados en la lucha contra este tipo de delitos.

Por otro lado, el reglamento en su artículo 23.1[9] y 23.2[10] también establece la utilización de herramientas tecnológicas avanzadas para el intercambio de información y la colaboración entre las autoridades. Esto incluye el uso de sistemas seguros de comunicación, plataformas compartidas para el análisis de datos y la interoperabilidad de bases de datos. Estas herramientas tecnológicas agilizan los procesos de cooperación, facilitan el intercambio de información en tiempo real y mejoran la eficiencia de las investigaciones.

En conclusión, los mecanismos de cooperación establecidos en las normativas que respaldan la actuación de Eurojust en la lucha contra el cibercrimen transfronterizo son fundamentales para enfrentar de manera eficaz esta creciente amenaza. La designación de puntos de contacto, el intercambio de información, la coordinación de investigaciones, la realización de operaciones conjuntas y el uso de herramientas tecnológicas, son elementos clave que permiten una colaboración más estrecha entre las autoridades competentes de los Estados miembros. Estos mecanismos fortalecen la capacidad de respuesta contra el cibercrimen, mejoran la prevención y persecución de los delitos cibernéticos, y contribuyen a garantizar la seguridad digital en la Unión Europea y más allá.

3.1.2. Análisis del Convenio de Budapest sobre ciberdelincuencia

El Convenio de Budapest[11] es un tratado internacional que ha sido ratificado por varios países europeos. Actualmente son 68 los Estados Parte del convenio y 20 los observadores. Establece un marco legal para la cooperación transfronteriza en la lucha contra el cibercrimen.

[9] Artículo 21.1 del Reglamento (UE) 2018/1727 sobre Eurojust: “Eurojust creará un sistema de gestión de casos compuesto de expedientes temporales de trabajo y un índice que contendrá datos personales, tal como se contempla en el anexo II, y no personales.”.

[10] Artículo 21.1 del Reglamento (UE) 2018/1727 sobre Eurojust: “El sistema de gestión de casos tendrá por objeto: a) servir de ayuda para la gestión y la coordinación de las investigaciones y procesos penales a los que Eurojust proporciona asistencia, en particular mediante el cotejo de datos; b) facilitar el acceso a la información sobre las investigaciones y procesos penales en curso; c) facilitar el control de la licitud del tratamiento de los datos personales de Eurojust y su cumplimiento con las normas de protección de datos aplicables”.

[11] Se ha de precisar que el Convenio de Budapest sobre la cibercriminalidad fue celebrado el 23 de noviembre de 2001 por parte del Consejo de Europa, y no es una normativa propia de la Unión Europea.

El Convenio sobre la Cibercriminalidad está compuesto por 48 artículos y un preámbulo inicial. Está organizado en cuatro capítulos con secciones y títulos. El primer capítulo se enfoca en la terminología utilizada en el texto. El segundo capítulo, llamado "Medidas que deberán adoptarse a nivel nacional", abarca aspectos tanto del derecho material (responsabilidad penal, tentativa, complicidad, entre otros) como del derecho procesal (procedimientos, salvaguardias, datos, registros, jurisdicción, entre otros). El tercer capítulo se centra en la cooperación internacional, e incluye temas como la extradición, la asistencia entre Estados, el intercambio de información y datos, y el establecimiento de una red de comunicación disponible las 24 horas del día, los 7 días de la semana. El último capítulo contiene las disposiciones finales propias de un tratado internacional, como la adhesión, la entrada en vigor, la aplicación territorial, los efectos, el régimen de reservas, las denuncias, las notificaciones, entre otros (Díaz Gómez, 2010).

Desde el punto de vista de Díaz Gomez (2010), la extensión supranacional tiene un papel vital en el tratamiento de los delitos informáticos. Una de las ideas más importantes es abarcar el mayor número posible de Estados a través de políticas basadas en la cooperación internacional: "Lo ideal no son los Tratados bilaterales, sino convenios multilaterales que involucren al mayor número de países posible. De este modo sería posible armonizar las políticas regionales en materia de cibercrímenes, logrando una regulación coherente, que no se contradiga y cuya utilización fuera posible a gran escala." (Díaz Gómez, 2010, p. 183).

El Convenio de Budapest sobre Ciberdelincuencia representa una materialización concreta de muchas de las ideas discutidas anteriormente, ya que promueve y facilita la cooperación en el ámbito de los delitos informáticos a nivel internacional. Este convenio es considerado como uno de los instrumentos más completos y efectivos en la lucha contra el cibercrimen, abarcando una amplia gama de delitos cibernéticos, y estableciendo normas y procedimientos para su prevención y persecución (Díaz Gómez, 2010).

En términos simples, el convenio busca maximizar la cooperación entre los países en la lucha contra los delitos informáticos. Proporciona un marco legal sólido para que los países compartan información, brinden asistencia mutua y coordinen sus esfuerzos en la investigación y persecución de los delitos cibernéticos. Esto se traduce en una mayor colaboración y coordinación entre las autoridades competentes de diferentes países, lo que permite una respuesta más eficaz y eficiente ante los desafíos que plantea el cibercrimen en la actualidad.

El espíritu de cooperación internacional con el que fue elaborado el citado convenio está plasmado en su Capítulo III "Cooperación Internacional". En su artículo 23[12] se describe como las partes estarán de acuerdo en cooperar y utilizar todos los medios disponibles para trabajar en conjunto en la lucha contra el crimen. Esto implica seguir los acuerdos y tratados internacionales relacionados con la cooperación penal, así como utilizar su propia legislación nacional para facilitar la colaboración y el intercambio de información en casos penales transfronterizos.

Sumado a lo anterior, merece la pena destacar el contenido relativo a la asistencia mutua del artículo 25.1[13]. En este punto se establece que las partes involucradas se comprometen a brindar asistencia mutua en casos de investigaciones o procedimientos relacionados con delitos relacionados con sistemas y datos informáticos. Esto incluye la obtención de pruebas en formato electrónico de un delito. En otras palabras, si una parte necesita ayuda en una investigación o proceso relacionado con delitos informáticos, las otras partes se comprometen a brindar la asistencia necesaria en la medida de sus posibilidades.

[12] Artículo 23 del Convenio de Budapest sobre la ciberdelincuencia del 23 de noviembre de 2001: "Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.".

[13] Artículo 25.1 del Convenio de Budapest sobre la ciberdelincuencia del 23 de noviembre de 2001: "Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.".

La implicación de otras áreas del sistema legal, lo hacen mucho más completo. Esto se refleja en la flexibilización de las medidas que los Estados deben tomar, no limitándose únicamente a las acciones legislativas, sino también considerando otras acciones (Díaz Gómez, 2010).

Otro aspecto importante a remarcar es que el Convenio sobre cibercriminalidad es una iniciativa del Consejo de Europa, y por lo tanto, su alcance no se limita solo a los Estados miembros de dicho Consejo. De acuerdo con el artículo 37[14] del Convenio, otros Estados también tienen la posibilidad de ratificarlo. Esto facilita avanzar hacia un nivel de reconocimiento internacional necesario para abordar eficazmente los desafíos en el ámbito de la cibercriminalidad (Díaz Gómez, 2010).

Entre las numerosas críticas de Díaz Gómez (2010) podemos destacar aquellas relacionadas con la armonización de los delitos cibernéticos, el adecuado uso de las leyes y la colaboración policial para combatir el cibercrimen, concretamente en relación con el intercambio de datos e información.

3.1.3. Análisis comparativo entre el marco legal de Eurojust y el Convenio de Budapest sobre ciberdelincuencia

Una vez examinados los marcos legales en los epígrafes anteriores, se procederá a realizar un análisis comparativo entre el marco legal de Eurojust y el Convenio de Budapest sobre ciberdelincuencia.

El análisis comparativo se realizará en función de los siguientes criterios: alcance geográfico y jurisdiccional, enfoque del ciberdelito, cooperación y asistencia legal.

[14] Artículo 37 del Convenio de Budapest sobre la ciberdelincuencia del 23 de noviembre de 2001: “1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros. 2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.”.

3.1.3.1. Alcance geográfico y jurisdiccional

El Convenio de Budapest es un acuerdo internacional del Consejo de Europa que destaca por su gran alcance geográfico global. A diferencia del Reglamento Eurojust, que se aplica sólo a los Estados miembros de la Unión Europea, el Convenio de Budapest está abierto a la firma y ratificación de países no europeos. Esto quiere decir que su alcance se expandirá internacionalmente, permitiendo la participación de países de todo el mundo. Este ámbito geográfico es decisivo en la lucha contra el ciberdelito, que trasciende las fronteras nacionales y requiere una cooperación internacional eficaz.

En cuanto a la jurisdicción, el Convenio de Budapest establece que los Estados Partes pueden establecer jurisdicción sobre los delitos cibernéticos cometidos contra los sistemas informáticos o la información, cometidos o ubicados dentro de su territorio. Permite a los países investigar y enjuiciar los delitos cibernéticos dentro de su propia jurisdicción. El enfoque del acuerdo en el ciberdelito aumenta la importancia de la acción coordinada a nivel nacional para prevenir, investigar y sancionar los delitos en el sector digital (Díaz Gómez, 2010).

No obstante, el ámbito geográfico del Reglamento Eurojust es más reducido, ya que concierne exclusivamente a los Estados miembros de la Unión Europea. Aunque esto limita su ámbito territorial a la UE, también facilita una cooperación más estrecha y flexible entre los Estados miembros en la lucha contra los delitos internacionales graves. Centrándose en la cooperación dentro de la UE en Derecho Penal, el Reglamento Eurojust tiene como objetivo promover la coordinación y el intercambio de información entre las autoridades judiciales de los Estados miembros en relación con delitos internacionales como el terrorismo, el tráfico de drogas y otros delitos graves. Este enfoque es coherente con la necesidad de responder a los desafíos jurídicos y de seguridad específicos de la UE (Pérez Souto, 2013).

El Convenio de Budapest tiene un alcance geográfico más amplio y se ocupa específicamente de la ciberdelincuencia, mientras que el Reglamento de Eurojust se

centra en la cooperación internacional en materia de justicia penal dentro de la UE para combatir una amplia gama de delitos graves. Ambas herramientas son importantes en la lucha contra el crimen internacional, ya que se adaptan a las necesidades y circunstancias específicas.

3.1.3.2. Enfoque del ciberdelito

El Convenio de Budapest destaca por su enfoque específico en el ciberdelito. Fue creado con el objetivo de abordar los delitos informáticos y las infracciones relacionadas con estos. Este convenio define y penaliza una amplia gama de ciberdelitos, como el acceso no autorizado a sistemas informáticos, el sabotaje informático, el fraude informático y la pornografía infantil en línea. Por este motivo, su objetivo principal es armonizar las leyes y fortalecer la cooperación internacional para combatir eficazmente el ciberdelito.

Esta afirmación se puede fundar en la forma en la que algunos de sus artículos están elaborados o el contenido de los mismos. Por ejemplo, el artículo 1[15] del mencionado convenio establece la terminología en el que se incluyen las definiciones de sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico. Más ejemplos de esta cuestión se pueden apreciar en el artículo 2 y siguientes, haciendo referencia a los accesos ilícitos, interferencia de datos, abuso de los dispositivos, fraude informático etc.

[15] Artículo 1 del Convenio de Budapest sobre la Ciberdelincuencia del 23 de noviembre de 2001:
"a) Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;
b) por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;
c) por «proveedor de servicios» se entenderá:
i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y
ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;
d) por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.".

Tal y como sostiene Díaz Gomez (2010) es cada vez más común el expansionismo del Derecho Penal, al ser un fenómeno global que se está incorporando gradualmente en todos los países y en sus respectivas jurisdicciones penales, donde además el ámbito informático se hace cada vez más necesario, por la aparición de nuevos bienes jurídicos y riesgos.

En contraposición, el Reglamento de Eurojust no se centra única y exclusivamente en el ciberdelito, sino en la cooperación judicial penal transnacional a un nivel más general. Aunque el ciberdelito puede ser abordado por Eurojust en casos concretos, su enfoque es más amplio y abarca diversos delitos graves que trascienden al ámbito digital, como el terrorismo, el tráfico de drogas y el crimen organizado. El Reglamento de Eurojust busca facilitar la coordinación y el intercambio de información entre las autoridades judiciales de los Estados miembros de la Unión Europea, para combatir eficazmente la delincuencia transnacional en todas sus formas (Pérez Souto, 2013).

Es precisamente esta diferencia la que puede causar dificultades a la hora de la persecución de los ciberdelitos, al existir obstáculos en la armonización entre ambos instrumentos legales. Cada Estado tiene un sistema legal propio y normas específicas, por lo que la diferencia de enfoques podría llegar a generar problemas, por ejemplo en la forma y modo en la que se realizan las investigaciones y acciones judiciales. Esto podría también producir una falta de orientación clara y precisa sobre cómo coordinar los medios y recursos que se encuentran a disposición de cada Estado, lo que afectaría negativamente a la cooperación y eficacia en la lucha contra el cibercrimen transnacional.

3.1.3.3. Cooperación y asistencia legal entre Estados miembros

Para concluir este análisis, la cooperación y asistencia legal entre Estados miembros también presenta diferencias sustanciales.

Primeramente, la estructura institucional de Eurojust facilita mucho más la cooperación judicial entre los Estados miembros al contar con un marco legal sólido

respaldado por la Unión Europea (UE). Esto se ha traducido en el establecimiento de relaciones funcionales que producen un mejor aprovechamiento de los recursos que se encuentran disponibles, evitando de esta forma duplicidades y un mal funcionamiento (Alonso Moreda, 2012).

Ejemplos de lo mencionado pueden apreciarse en las relaciones de Eurojust con actores como Europol, la Red Judicial Europea (RJE) y la Oficina Europea de Lucha contra el Fraude (OLAF)[16], creando un espacio y una red de cooperación judicial internacional ágil y eficaz. De hecho, la redacción del reglamento del Eurojust está inspirada en la importancia de las relaciones funcionales entre el Eurojust y los demás actores (Alonso Moreda, 2012).

Por esta razón, "[...] la legislación europea se presenta como adalid indiscutible de las nuevas formas de colaboración entre Estados" (Díaz Gómez, 2010, p. 184), calificando así a las formas de participación y contribución entre Estados.

En cambio, el Convenio de Budapest puede presentar dificultades, como por ejemplo, en las barreras lingüísticas y culturales debido a la diversidad en idiomas y prácticas legales de los diferentes Estados miembros. A estas dificultades se suma la falta de armonización legislativa. Aunque el Convenio de Budapest establece un marco para la cooperación en delitos informáticos, la implementación por parte de los países miembros sigue siendo un problema sustancial (Díaz Gómez, 2010).

Aún así, el Convenio de Budapest tiene aspectos positivos en este apartado, como los procesos en los que se comparten información, experiencias y buenas prácticas, así como determinadas herramientas adicionales y aceleradas para mejorar la cooperación y la divulgación de pruebas electrónicas.

[16] OLAF, la Oficina Europea de Lucha contra el Fraude, es el nombre utilizado en las fuentes y medios oficiales de la Unión Europea, tanto en español como en inglés, ya que el significado de sus siglas proviene de su nombre en francés *Office de Lutte Anti-Fraude*.

3.2. Funciones y competencias de Eurojust en la cooperación judicial contra el cibercrimen

3.2.1. Cambios en las funciones y competencias de Eurojust en la transición de la Decisión 2002/187/JAI del Consejo al Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal

Como ya se ha mencionado en epígrafes anteriores, la Decisión 2002/187/JAI del Consejo creó Eurojust con el objetivo de mejorar y fortalecer la cooperación y coordinación entre las autoridades judiciales competentes de los Estados miembros, especialmente en casos de delincuencia organizada grave.

La Comisión encargó un estudio externo que fue presentado en 2012 cuya propuesta relacionada con el Eurojust era la reforma de este, teniendo como base el artículo 85 del Tratado de Funcionamiento de la Unión Europea (TFUE). No fue hasta junio de 2018 cuando se llegó a un acuerdo provisional para la reforma de Eurojust, y su aprobación final en noviembre del mismo año. Hay que tener en cuenta que la base legal de los Tratados que son aplicables a Eurojust está presente en el artículo 85 del TFUE (Hernández López, 2020).

El artículo 85.1[17] del TFUE describe la función de Eurojust, haciendo énfasis en su componente de apoyo y de refuerzo en la coordinación y cooperación entre las

[17] Artículo 85.1 del TFUE: “La función de Eurojust es apoyar y reforzar la coordinación y la cooperación entre las autoridades nacionales encargadas de investigar y perseguir la delincuencia grave que afecte a dos o más Estados miembros o que deba perseguirse según criterios comunes, basándose en las operaciones efectuadas y en la información proporcionada por las autoridades de los Estados miembros y por Europol. A tal fin, el Parlamento Europeo y el Consejo determinarán, mediante reglamentos adoptados con arreglo al procedimiento legislativo ordinario, la estructura, el funcionamiento, el ámbito de actuación y las competencias de Eurojust. Estas competencias podrán incluir:
a) el inicio de diligencias de investigación penal, así como la propuesta de incoación de procedimientos penales por las autoridades nacionales competentes, en particular los relativos a infracciones que perjudiquen a los intereses financieros de la Unión;
b) la coordinación de las investigaciones y los procedimientos mencionados en la letra a);
c) la intensificación de la cooperación judicial, entre otras cosas mediante la resolución de conflictos de jurisdicción y una estrecha cooperación con la Red Judicial Europea.
En dichos reglamentos se determinará asimismo el procedimiento de participación del Parlamento Europeo y de los Parlamentos nacionales en la evaluación de las actividades de Eurojust.”.

autoridades nacionales, cuando sean dos o más los Estados miembros afectados por delincuencia grave. Es precisamente en el párrafo segundo de este artículo donde se presentan las novedades del reglamento aprobado, gracias a las cuales las reformas posibles y futuras reformas de Eurojust no requerirán la aprobación por unanimidad del Consejo, al realizarse a partir de ese momento por el procedimiento legislativo ordinario, es decir, que en caso de que requiera una votación, se decidirá por mayoría simple (Hernández López, 2020).

Además, el art. 85.1 establece y reconoce tres tipos de competencias para Eurojust siendo estas el inicio de diligencias de investigación penal y la proposición de incoación de procedimientos penales, su coordinación, y la intensificación de la cooperación judicial.

En la misma línea, las principales novedades introducidas por el Reglamento (UE) 2018/1727 tienen que ver con la forma y modo en el que Eurojust lleva a cabo sus funciones. Esto es realmente importante ya que hasta el momento, Eurojust solo podía desempeñar sus funciones previa solicitud expresa de una de las autoridades nacionales competentes implicadas en el asunto. De esta manera, se proporcionó a Eurojust con una gran capacidad de iniciativa propia para poder intervenir (Hernández López, 2020).

Sumado a lo anterior, todas las solicitudes válidas de autoridades competentes de los Estados miembros deberán ser examinadas y respondidas por Eurojust. También es importante que se considere cualquier información proporcionada por las autoridades y entidades competentes de la Unión Europea con respecto a las disposiciones adoptadas en el marco de los Tratados. En último lugar, otra novedad importante es el cambio en la estructura de Eurojust. Además de estar compuesto por los miembros nacionales, se establece un Colegio (compuesto por todos los miembros nacionales y un representante de la Comisión), un Consejo Ejecutivo y un director administrativo (Alonso Salgado, 2019).

3.2.2. Análisis de las funciones

Las funciones de Eurojust se encuentran recogidas en el artículo 2, que se encuentra dividido en tres apartados diferenciados.

En el primer apartado, el art. 2.1[18] refleja como Eurojust tiene la función de respaldar y fortalecer la coordinación y cooperación entre las autoridades nacionales, responsables de investigar y perseguir delitos graves que estén dentro de su competencia, siempre y cuando dichos delitos afecten a dos o más Estados miembros o deban ser perseguidos de acuerdo con criterios comunes.

En el segundo apartado correspondiente al art. 2.2[19] dispone dos cuestiones: la primera, a través de la cual Eurojust considerará cualquier solicitud de las autoridades competentes de los Estados miembros, así como la información facilitada por las autoridades, agencias, organizaciones y organismos de la Unión; y la segunda, según la cual se tendrá en cuenta el principio de reconocimiento mutuo y se facilitará la ejecución de las solicitudes y decisiones en materia de cooperación judicial.

En el tercer y último apartado, el art. 2.3[20] establece la independencia, que nace fruto de la implementación del Reglamento (UE) 2018/1727, y que le otorga la

[18] Artículo 2.1 del Reglamento (UE) 2018/1727 sobre Eurojust: "Eurojust apoyará y reforzará la coordinación y la cooperación entre las autoridades nacionales encargadas de investigar y perseguir las formas de delincuencia grave para la que Eurojust sea competente de conformidad con el artículo 3, apartados 1 y 3, cuando dichas formas de afecten a dos o más Estados miembros o deban perseguirse según criterios comunes, basándose en las operaciones efectuadas y en la información proporcionada por las autoridades de los Estados miembros, por Europol, por la Fiscalía Europea y por la OLAF.".

[19] Artículo 2.2 del Reglamento (UE) 2018/1727 sobre Eurojust:."En el desempeño de sus funciones, Eurojust: a) tendrá en cuenta cualquier solicitud procedente de una autoridad competente de un Estado miembro, cualquier información facilitada por autoridades, instituciones, órganos, organismos y agencias de la Unión competentes en virtud de disposiciones adoptadas en el marco de los Tratados y cualquier información recopilada por el propio Eurojust; b) facilitará la ejecución de las solicitudes y decisiones en materia de cooperación judicial, incluidas las solicitudes y decisiones basadas en instrumentos que den efecto al principio de reconocimiento mutuo.".

[20] Artículo 2.3 del Reglamento (UE) 2018/1727 sobre Eurojust: "Eurojust desempeñará sus funciones a petición de las autoridades competentes de los Estados miembros o por propia iniciativa, o a petición de la Fiscalía Europea dentro de los límites de la competencia de la Fiscalía Europea.".

facultad de desarrollar sus funciones por petición de las autoridades competentes de los Estados miembros, por propia iniciativa, o a petición de la Fiscalía Europea.

En los artículos 4 y 5 del reglamento se contienen las funciones operativas y el desempeño de estas y otras funciones. A modo de síntesis, en el art. 4.1 hace una recopilación de todas las funciones operativas que Eurojust debe llevar a cabo, siendo algunas de estas la asistencia a las autoridades competentes de los Estados, para mejorar la coordinación en las investigaciones y procesos, la asistencia para mejorar la cooperación en los análisis realizados, el apoyo a los centros de asesoramiento especializados de la Unión, el apoyo a la acción de los Estados para combatir las formas de delincuencia grave, y la cooperación estrecha con la Fiscalía Europea en asuntos de su competencia.

Además, en el art. 4.2 se menciona que Eurojust tiene la capacidad de solicitar a las autoridades competentes de los Estados miembros que investiguen o persigan hechos concretos, que acepten que las mismas autoridades se encuentran más capacitadas para perseguir unos hechos concretos, que se realice una coordinación entre autoridades de Estados miembros afectados o se constituya un equipo conjunto de investigación, que faciliten toda la información necesaria, que se tomen medidas especiales para investigar o que tomen otra medida que pueda estar justificada para la persecución o investigación (siempre y cuando la solicitud esté motivada). Eurojust también tiene la capacidad de poder facilitar a la Europol dictámenes y de facilitar apoyo logístico, tal y como figura en el art. 4.3.

En cuanto al desempeño de las funciones operativas del artículo 5, se establecen dos formas[21] de actuación por parte de Eurojust, siendo la primera de estas a través de uno o varios de los miembros afectados, y la segunda de manera colegiada.

Una vez analizadas todas las funciones, podemos concluir que las funciones que posee Eurojust son muy diversas y se basan en la coordinación y apoyo a las

[21] En el artículo 5 del Reglamento (UE) 2018/1727 sobre Eurojust se detallan las situaciones en las que Eurojust tendrá que actuar de un modo u otro, siendo estas las mencionadas en el análisis (a través de miembros nacionales o colegiadamente).

investigaciones y enjuiciamientos transfronterizos, el fomento de la cooperación operativa entre Estados miembros, la facilitación en el intercambio de información y la ejecución de medidas coercitivas. Todas estas funciones son posibles gracias a la gran independencia y capacidad de iniciativa, aunque no total y absoluta, con la que cuenta la agencia.

De hecho, Alonso Moreda (2012) considera que la celebración de las reuniones[22] operativas, que derivan precisamente de estas funciones, son el principal instrumento de trabajo de Eurojust. Uno de estos indicativos de lo relevantes que pueden llegar a ser, es la frecuencia cada vez mayor con la que se celebran estas reuniones.

3.2.3. Análisis de las competencias

Las competencias de Eurojust se encuentran enumeradas en el artículo 3, denominado "Competencias de Eurojust" perteneciente al Reglamento (UE) 2018/1727. El art. 3 contiene seis apartados, los cuales serán objeto de análisis de este epígrafe.

El art. 3.1[23] se encarga de establecer las formas de delincuencia grave respecto a las cuales Eurojust será competente. Estas formas de delincuencia grave se encuentran enumeradas en el Anexo I del reglamento. De entre todas las formas de delincuencia graves que se encuentran en el mencionado Anexo I, podemos destacar, en relación con el objeto del presente trabajo de investigación, la ciberdelincuencia, la delincuencia organizada, las actividades de blanqueo de capitales, la estafa y el fraude, delitos contra los intereses financieros de la Unión, falsificación y piratería.

También cabe mencionar que en el propio artículo 3.1 se matiza que desde el momento en el que la Fiscalía Europea asuma las funciones de investigación y

[22] Las reuniones operativas tienen lugar en la sede de Eurojust, aunque en ocasiones se celebran en uno de los Estados afectados.

[23] El anexo I mencionado en el artículo 3.1 del Reglamento (UE) 2018/1727 sobre Eurojust, se encuentra al final del mismo, en él se enumeran hasta treinta tipos diferentes de delincuencia grave.

acusación, Eurojust no podrá ejercer su competencia respecto a los delitos en los que sea competente esta. De este modo queda limitada la acción de Eurojust, aunque se contempla como excepción aquellos casos en los que los Estados que se encuentran afectados no han participado en la cooperación reforzada para la creación de la Fiscalía por petición propia, o la Fiscalía Europea decida no participar (Escalada López, 2023).

A partir del art. 3.2 y hasta el art. 3.6 se realizan una serie de consideraciones según las cuales Eurojust podrá ser o no competente para conocer determinados delitos en función de las condiciones que tengan lugar. De esta manera el art. 3.2 establece que Eurojust podrá ejercer su competencia en aquellos delitos que afecten a los interes financieros de la Unión, pero con el matiz de que los países que se hallen implicados, hayan tenido que participar en la cooperación reforzada para la creación de la Fiscalía Europea, y esta no tenga competencia o haya decidido no ejercerla. Del mismo modo, en los arts. 3.3 y 3.5 queda reflejado que Eurojust podrá, con arreglo a sus funciones, colaborar en actuaciones judiciales e investigaciones a instancia de una autoridad competente, o bien a petición de una autoridad competente de un Estado miembro, que posibilite el apoyo de Eurojust en las investigaciones e incoación de procesos penales que afecten a dicho Estado.

Otra cuestión parecida aunque también con ciertos matices, es la planteada en el art. 3.6, ya que se establece que aunque a petición de una autoridad competente de un Estado miembro o de la Comisión, se posibilite a Eurojust prestar apoyo a las investigación y a la incoación de procesos penales, es importante que estos tengan repercusiones a escala de la Unión, existiendo la obligación de consultar previamente al desarrollo de las labores de apoyo e investigación a la autoridad competente.

De este modo, la operatividad inicial y las competencias de Eurojust quedan ciertamente delimitadas, "[...] previa solicitud de la Comisión o de un Estado miembro, la función de apoyo a las investigaciones y actuaciones judiciales podrá referirse a procesos penales que afecten exclusivamente al Estado Miembro en

cuestión pero tengan repercusión a escala de la Unión" (Escalada López, 2023, p. 489). Sumado a esto, puede también darse el caso de que afecten al Estado en cuestión, o a un tercer Estado en el que exista un acuerdo de cooperación con Eurojust.

3.3. Análisis de la eficacia de Eurojust en la cooperación judicial internacional en casos de cibercrimen transfronterizo

3.3.1. Evaluación de la operación *Avalanche*

3.3.1.1. Breve introducción al caso

Se llevó a cabo una investigación alemana sobre una organización criminal en línea llamada *Avalanche*, que estaba involucrada en campañas de *malware* y *phishing*. Comenzó en 2012 después de que una ola de *ransomware*[24] infectara numerosos sistemas informáticos y bloqueara el acceso de los usuarios. La infraestructura de *Avalanche* estaba configurada para ser altamente resistente a los cierres y la acción de las fuerzas del orden. La investigación descubrió la existencia de una infraestructura tecnológica sofisticada, utilizada para infectar millones de sistemas informáticos personales y comerciales con *malware*[25], como troyanos bancarios y *ransomware* (European Union Agency for Criminal Justice Cooperation, 2017).

Esto dio lugar al robo de contraseñas bancarias y contraseñas de correo electrónico por parte de los delincuentes que gestionan la red. Con esta información, los delincuentes pudieron realizar transferencias bancarias desde las cuentas de las víctimas. Además, los fondos se canalizaron hacia los delincuentes a través de una infraestructura diseñada específicamente para asegurar el producto de sus actividades delictivas (European Union Agency for Criminal Justice Cooperation, 2017).

[24] *Ransomware* es un tipo de malware que impide que los usuarios accedan a su sistema y archivos personales y exige el pago de un rescate para recuperar el acceso. Se considera un secuestro de datos.
[25] *Malware* es un programa malicioso.

3.3.1.2. Impacto producido y el papel de Eurojust en el caso

La infraestructura de *Avalanche* ha estado en uso desde 2009, y causó daños significativos en el sistema bancario en línea de Alemania, estimados en seis millones de euros. Además, los ataques de *malware* realizados a través de la red de *Avalanche*, han resultado en pérdidas económicas que se estiman en cientos de millones de euros a nivel mundial. Sin embargo, debido a la gran cantidad de tipos de *malware* gestionados en la plataforma de *Avalanche*, es difícil calcular el número exacto de las pérdidas (European Union Agency for Criminal Justice Cooperation, 2017).

Inicialmente, se había programado una fecha de acción para 2015, pero se pospuso hasta finales de 2016 para colaborar estrechamente con las autoridades estadounidenses y así identificar a los responsables. Surgieron preocupaciones sobre la soberanía, debido a la ubicación de los servidores que se iban a desmantelar en diferentes jurisdicciones, pero las discusiones entre las autoridades pertinentes resolvieron el problema. También se planteó el problema de que en algunos países participantes no fuera posible la confiscación de los dominios que aún no estaban activos. Sin embargo, los expertos en ciberdelincuencia de Eurojust pudieron informar a las autoridades nacionales que este problema no surgiría, ya que el estado de los dominios en cuestión cambiaría de no activos a activos en el momento de llevar a cabo las acciones (European Union Agency for Criminal Justice Cooperation, 2017).

Se desempeñó un papel de asesoramiento constante para la Oficina Nacional y las autoridades nacionales a lo largo de la investigación. Además, se proporcionaron los detalles de contacto de las autoridades judiciales en países que no formaban parte de la red de contactos de Eurojust. Eurojust apoyó el trabajo de las autoridades judiciales pertinentes al establecer los requisitos legales para implementar las intervenciones necesarias, y facilitar la preparación e implementación oportunas de las solicitudes de las cartas rogatorias (European Union Agency for Criminal Justice Cooperation, 2017).

La Operación *Avalanche* demostró cómo las autoridades y sus divisiones de delitos cibernéticos competentes, han logrado un progreso vertical en su capacidad para comprender y neutralizar una amplia variedad de actividades delictivas tecnológicamente avanzadas. Los organismos encargados de hacer cumplir la ley están desarrollando continuamente enfoques innovadores para responder a las amenazas cibernéticas globales, como lo demuestra Europol y su Centro Europeo especializado en Delitos Cibernéticos (EC3). En particular, la destrucción del anillo cibernético *Avalanche* representa el mayor uso registrado de *sinkholing*[26]. La operación tuvo un alcance sin precedentes, con más de 800.000 dominios confiscados, destruidos o bloqueados. Debido al tamaño y alcance global de la red, la operación interrumpió temporalmente el ecosistema global de ciberdelincuencia (Wainwright & Cilluffo, 2017).

3.3.1.3. Resultados finales

Para la evaluación de los resultados finales del caso analizado, se ha considerado adecuado la elaboración de una tabla, estableciendo cinco aspectos a evaluar y cinco criterios correspondientes a estos, para determinar si Eurojust es eficaz en la lucha contra el crimen transfronterizo. La puntuación oscila entre 1 y 5, siendo 1 el valor mínimo y 5 el valor máximo.

[26] *Sinkholing es una* tecnología utilizada para combatir la infraestructura del ciberdelincuente interfiriendo los canales de comando y control.

Tabla 1

Análisis crítico de la eficacia de Eurojust en la Operación Avalanche

Aspecto a evaluar	Criterio aplicado	Puntuación (1-5)
Objetivos	Cumplimiento de objetivos establecidos	5
Impacto	Reducción del delito o amenaza del cibercrimen	3
Colaboración	Nivel de cooperación y coordinación entre agencias y países	4
Medidas de prevención	Implementación de medidas para prevenir futuros ciberdelitos	3
Recursos utilizados	Eficacia en la asignación y utilización de recursos	4
Evaluación	Eficacia global de la operación	19 (eficaz)

Nota: la puntuación total máxima posible es de 25. Si la puntuación total es mayor o igual a 20 se considerará “altamente eficaz”. Si la puntuación total es menor a 20 pero mayor o igual a 15 se considerará “eficaz”. Si la puntuación total es menor a 15 pero mayor o igual a 10 se considerará “moderadamente eficaz”. Si la puntuación total es menor a 10 se considerará “ineficaz”.
Fuente: elaboración propia con base en datos de (European Union Agency for Criminal Justice Cooperation, 2017).

En cuanto a la justificación de las puntuaciones asignadas:

- Objetivos: se ha asignado un valor de 5 en función del criterio aplicado “cumplimiento de objetivos establecidos” para evaluar este aspecto. El motivo se debe a que el objetivo establecido fue eliminar la amenaza de *malware* y *phishing*, y teniendo en cuenta que esta amenaza fue completamente neutralizada, se le ha asignado la máxima puntuación.

- Impacto: se ha asignado un valor de 3 en función del criterio aplicado “reducción del delito o amenaza del cibercrimen” para evaluar este aspecto. El motivo se debe a que el impacto que tuvo esta operación redujo significativamente el cibercrimen de este tipo, si bien, actualmente siguen produciéndose casos de *malware y phishing*, pero a una escala menor.

- Colaboración: se ha asignado un valor de 4 en función del criterio aplicado “nivel de cooperación y coordinación entre agencias y países” para evaluar este aspecto. El motivo se debe a que la cooperación entre agencias como Eurojust y Europol fue excelente, aunque el nivel de cooperación entre los países y estas agencias no fue tan bueno.

- Medidas de prevención: se ha asignado un valor de 3 en función del criterio aplicado “implementación de medidas para prevenir futuros ciberdelitos” para evaluar este aspecto. El motivo se debe a que la prevención que existía en estos años no era tan elevada como la que tenemos a día de hoy, por las reformas legislativas y la mejora que ha habido en la cooperación judicial. Aún así, las distintas agencias y organismos estaban dotadas con mecanismos de prevención y disuasión para evitar que el resultado fuera más negativo todavía.

- Recursos utilizados: se ha asignado un valor de 4 en función del criterio aplicado “eficacia en la asignación y utilización de recursos” para evaluar este aspecto. El motivo se debe a que los recursos fueron utilizados y asignados de manera apropiada, si bien existieron ciertos problemas con el sector privado a la hora de poder asignar ciertos recursos en el tratamiento y análisis de datos, tal y como figura en el informe.

Conforme a los objetivos, criterios y puntuaciones fijados, la evaluación final es de 19 puntos sobre 25, considerando esta operación como eficaz, de acuerdo con los parámetros establecidos.

3.3.2. Evaluación de la operación *BlackShades*

3.3.2.1. Breve introducción al caso

BlackShades era una organización que desarrollaba y vendía *malware*, y que permitía a los compradores infectar y controlar ordenadores de forma remota, incluida la realización de ataques cibernéticos de denegación de servicio distribuido [27] (DDoS). Las investigaciones revelaron vínculos con varios Estados miembros. En los Países Bajos, un ejemplo del uso de *malware* con fines delictivos fue un caso en el que un hombre de 18 años infectó al menos 2.000 ordenadores al monitorear las cámaras web de las víctimas para grabar a mujeres y niñas (European Union Agency for Criminal Justice Cooperation, 2015).

Se contactó con Eurojust a través de un fiscal holandés que tenía contactos con diversas agencias de investigación y con la Oficina del Fiscal de Estados Unidos. Las autoridades estadounidenses tenían la intención de cerrar los servidores *BlackShades*, pero no tenían la intención de perseguir y enjuiciar a los ciudadanos extranjeros en Estados Unidos. El valor de la cooperación legal se hizo evidente cuando los autores, proveedores y usuarios del *malware BlackShades* fueron atacados por las fuerzas del orden y las agencias de aplicación de la ley, en 16 Estados durante esta investigación a nivel mundial. Se hizo así evidente el valor añadido de la cooperación judicial transfronteriza (European Union Agency for Criminal Justice Cooperation, 2015).

3.3.2.2. Impacto producido y el papel de Eurojust en el caso

El propósito de la primera conferencia de coordinación fue determinar qué Estados podrían emprender acciones legales contra las personas identificadas y considerar la posibilidad de acciones legales conjuntas entre los Estados involucrados. La reunión se celebró con relativa rapidez, pero contó con la presencia del país solicitante, las autoridades de Estados Unidos, Rumanía, Bélgica, Alemania y Francia, así como representantes de EC3 de Europol. Varios países realizaron sus

[27] Un ataque DDoS, o denegación de servicio distribuido, es un intento malicioso de interrumpir un servidor, servicio o tráfico de red y abrumar al objetivo o a la infraestructura circundante con una avalancha de tráfico de Internet.

propias investigaciones sobre este *malware* y reconocieron la necesidad de cooperación judicial internacional. Está claro que los países fuera de la conferencia también se vieron afectados, y por ello fueron invitados a conferencias posteriores (European Union Agency for Criminal Justice Cooperation, 2015).

La investigación culminó en una acción conjunta de dos días en mayo de 2014, coordinada por Eurojust a través de su Centro de Coordinación, con el apoyo de EC3. Durante los dos días de acción se realizaron 359 registros domiciliarios y 97 personas fueron detenidas. Se incautaron más de 1.100 dispositivos de almacenamiento de datos como ordenadores, portátiles, teléfonos móviles y discos duros externos sospechosos de ser utilizados para actividades ilegales. También se incautaron grandes cantidades de dinero en efectivo, armas de fuego ilegales y drogas. Las autoridades también se apoderaron con éxito del dominio del sitio web *BlackShades*. Los países que implementaron medidas fueron Holanda, Bélgica, Francia, Alemania, Reino Unido, Finlandia, Austria, Estonia, Dinamarca, Italia, Croacia, Estados Unidos, Canadá, Chile, Suiza y Moldavia (European Union Agency for Criminal Justice Cooperation, 2015).

Durante la operación, algunos usuarios inocentes, se vieron afectados por acciones gubernamentales, como la confiscación de dispositivos y el acceso a información personal bajo investigación. Estos daños colaterales perjudicaron a personas que no estuvieron directamente involucradas en la actividad delictiva. Otro impacto negativo fueron los pocos medios con los que contaban algunos Estados como Francia, que carecía de una Fiscalía especializada en delitos cibernéticos, lo que dificultó la coordinación al principio de la investigación (European Union Agency for Criminal Justice Cooperation, 2015). Las declaraciones de Eurojust dejan muy claro que la operación *Blackshades* fue satisfactoria por su magnitud y por el gran esfuerzo en la cooperación judicial transnacional que tuvo lugar: "Este caso, que involucra a tantos Estados miembros y terceros Estados, con el objetivo común de detener futuros ciberataques, muestra el potencial de las acciones conjuntas a nivel mundial y señala el camino hacia futuros esfuerzos comunes. Estamos muy satisfechos con

los resultados obtenidos." (European Union Agency for Criminal Justice Cooperation, 2015, p. 3).

3.3.2.3. Resultados finales

Para la evaluación de los resultados finales del caso analizado, se ha considerado adecuado la elaboración de una tabla, estableciendo cinco aspectos a evaluar y cinco criterios correspondientes a estos para determinar si Eurojust es eficaz en la lucha contra el crimen transfronterizo. La puntuación oscila entre 1 y 5, siendo 1 el valor mínimo y 5 el valor máximo.

Tabla 2

Análisis crítico de la eficacia de Eurojust en la Operación Blackshades

Aspecto a evaluar	Criterio aplicado	Puntuación (1-5)
Objetivos	Cumplimiento de objetivos establecidos	4
Impacto	Reducción del delito o amenaza del cibercrimen	3
Colaboración	Nivel de cooperación y coordinación entre agencias y países	4
Medidas de prevención	Implementación de medidas para prevenir futuros ciberdelitos	3
Recursos utilizados	Eficacia en la asignación y utilización de recursos	2
Evaluación	Eficacia global de la operación	16 (eficaz)

Nota: la puntuación total máxima posible es de 25. Si la puntuación total es mayor o igual a 20 se considerará “altamente eficaz”. Si la puntuación total es menor a 20 pero mayor o igual a 15 se considerará “eficaz”. Si la puntuación total es menor a 15 pero mayor o igual a 10 se considerará “moderadamente eficaz”. Si la puntuación total es menor a 10 se considerará “ineficaz”.

Fuente: elaboración propia con base en datos de (European Union Agency for Criminal Justice Cooperation, 2015).

En cuanto a la justificación de las puntuaciones asignadas:

- Objetivos: se ha asignado un valor de 4 en función del criterio aplicado “cumplimiento de objetivos establecidos” para evaluar este aspecto. El motivo se debe a que el objetivo establecido fue eliminar la amenaza que suponía *Blackshades*, y la cantidad de material y medios ilegales que proporcionaba. Teniendo en cuenta que esta amenaza fue neutralizada, aunque no en todos los países por igual, se le ha asignado esta puntuación.

- Impacto: se ha asignado un valor de 3 en función del criterio aplicado “reducción del delito o amenaza del cibercrimen” para evaluar este aspecto. El motivo se debe a que el impacto que tuvo esta operación redujo significativamente el cibercrimen de este tipo, si bien, actualmente siguen produciéndose casos parecidos a *Blackshades*. Además, en algunos países de aquel momento, *Blackshades* fue neutralizado, pero no se redujo la amenaza en la misma proporción en el resto.

- Colaboración: se ha asignado un valor de 4 en función del criterio aplicado “nivel de cooperación y coordinación entre agencias y países” para evaluar este aspecto. El motivo se debe a que la cooperación entre agencias como Eurojust, Europol y los departamentos de Estados Unidos y demás países de la Unión Europea fue extraordinaria, tal y como se ha mencionado anteriormente.

- Medidas de prevención: se ha asignado un valor de 3 en función del criterio aplicado “implementación de medidas para prevenir futuros ciberdelitos” para evaluar este aspecto. El motivo se debe a que muchos países se centraron en las medidas de represión y no tanto en las preventivas.

- Recursos utilizados: se ha asignado un valor de 2 en función del criterio aplicado “eficacia en la asignación y utilización de recursos” para evaluar este aspecto. El motivo se debe a que los recursos no fueron utilizados y asignados de manera apropiada, existiendo grandes diferencias entre los Estados a la hora de gestionar los mismos, lo que supuso un obstáculo adicional para neutralizar la amenaza.

Conforme a los objetivos, criterios y puntuaciones fijados, la evaluación final es de 16 puntos sobre 25, considerando esta operación como eficaz, de acuerdo con los parámetros establecidos.

3.4. Perspectivas de futuro y mejoras en la cooperación judicial internacional

3.4.1. Desafíos actuales y futuros en la cooperación judicial internacional contra el cibercrimen

El primero de los desafíos actuales que se han podido identificar es lo denominado como “geometría variable”. Este término se refiere a la flexibilidad o adaptabilidad en la forma en que las agencias gubernamentales interactúan y cooperan con las autoridades de su país. En lugar de seguir un enfoque único o estandarizado, la cooperación puede variar según el país y las circunstancias específicas. Esto significa que las agencias gubernamentales pueden establecer diversos niveles de cooperación y acuerdos de cooperación con varias autoridades nacionales en terceros países, dependiendo de factores como la naturaleza del caso, las relaciones bilaterales, los recursos disponibles y las políticas nacionales (Brière, 2018).

El problema de la geometría variable en la relación entre Eurojust y Europol, y las autoridades nacionales es de gran importancia, ya que la cooperación de las autoridades competentes es un factor clave para el éxito y el valor añadido de ambas agencias. Un ejemplo típico es la recopilación y difusión de información. Europol tiene bases de datos y herramientas técnicas a su disposición, pero depende de las autoridades nacionales de los Estados miembros, organismos de la

Unión, terceros países, organizaciones internacionales y entidades privadas para recopilar información. Las agencias gubernamentales pueden obtener y procesar información directamente, incluidos datos personales, solo de fuentes disponibles públicamente, como Internet y datos públicos (Brière, 2018).

Para solucionar este problema, Eurojust y las demás agencias así como los Estados miembros deben enfocarse en poder crear herramientas legales flexibles que ofrezcan las garantías suficientes, y en dotar a estas agencias de mayor libertad e independencia para poder adaptarse a los nuevos retos que se plantean, ya sea a través de modificaciones legales, creación de nuevos mecanismos de cooperación, el uso de las nuevas tecnologías o redes sociales, que podrían potenciar la colaboración entre Estados miembros como el análisis de *Big data*[28] y la inteligencia artificial. Todas estos medios pueden ser utilizados por Eurojust para identificar patrones, tendencias y conexiones en grandes volúmenes de información, lo que ayudaría a mejorar la capacidad de detección de delitos transfronterizos, y facilitaría la identificación de vínculos entre casos en diferentes Estados.

Otro de los retos y desafíos localizados, es el desarrollo cada vez mayor de un estatus diferenciado entre los Estados miembros de la UE. En general, la integración diferenciada se refiere a la diferenciación entre Estados miembros en la aplicación de la legislación de la Unión Europea. Esto se debe a la negativa de algunos Estados miembros a participar en el desarrollo del Derecho de la Unión en determinados ámbitos, y a su falta de voluntad para participar en dicha formulación (Brière, 2018).

La mayoría de los desafíos en casos de ciberdelitos se relacionan con la ejecución de solicitudes de asistencia legal mutua. Los retrasos en la ejecución de las solicitudes de asistencia legal mutua debido a la falta de coordinación entre las jurisdicciones afectadas por el delito o la negativa a ejecutar debido a conflictos de

[28] *Big data* se refiere a un amplio conjunto de datos que precisan de instrumentos y aplicaciones de índole informática para poder ser tratados y usados para un gran número de fines.

interés nacional o casos penales internos pendientes (European Union Agency for Criminal Justice Cooperation, 2020).

Según un informe de Eurojust (2020) el actual proceso de asistencia judicial recíproca se considera una forma lenta y engorrosa de recopilar y compartir datos electrónicos volátiles, por ejemplo, debido a la falta de coordinación entre las distintas jurisdicciones afectadas por la delincuencia. Además, la emisión y el cumplimiento de una solicitud de asistencia legal mutua pueden demorar más que el período legal de retención de datos del país solicitado.

Además, la emisión y el cumplimiento de la solicitud pueden llevar más tiempo del período legalmente establecido por la retención de datos en el país solicitado. Esto significa que, en muchos casos, el plazo para recopilar y compartir evidencia electrónica puede exceder el tiempo permitido para conservar esos datos según las leyes del país requerido. Esta discrepancia temporal puede dificultar la obtención de pruebas relevantes y comprometer la eficacia de las investigaciones transfronterizas (European Union Agency for Criminal Justice Cooperation, 2020).

3.4.2. Propuesta y desarrollo de una aplicación móvil

3.4.2.1. Justificación de la creación de la aplicación móvil

La justificación para la creación de la aplicación de Eurojust se basa en la necesidad de proporcionar a los usuarios una herramienta accesible y práctica que les permita acceder a información relevante sobre Eurojust, y a su trabajo en la lucha contra el cibercrimen transfronterizo en la Unión Europea, así como para estar al tanto de las cuestiones que atañen a la ciberseguridad, y facilitar un medio para resolver los problemas que puedan surgir con motivo de la ciberdelincuencia.

En primer lugar, Eurojust desempeña un papel fundamental en la cooperación judicial entre los Estados miembros de la UE en casos de delitos transfronterizos, incluido el ciberdelito. La creación de una aplicación dedicada a Eurojust permitiría a los usuarios acceder fácilmente a información sobre sus funciones y actividades.

Además, el ciberdelito es una amenaza en constante evolución que requiere una respuesta rápida y coordinada. Una aplicación de Eurojust podría proporcionar actualizaciones y noticias en tiempo real sobre los últimos desarrollos en materia de ciberseguridad, así como alertas sobre amenazas y consejos prácticos para protegerse contra ellas.

La aplicación también podría incluir una sección de contactos de emergencia de ciberseguridad, lo que permitiría a los usuarios acceder rápidamente a los recursos necesarios en caso de ser víctimas de un ciberataque, o presenciar actividades delictivas en línea, independientemente del país en el que se encuentren dentro de la Unión Europea y Reino Unido.

Además, la aplicación podría ofrecer información sobre el marco legal de Eurojust y su relación con la legislación nacional y de la UE en materia de ciberseguridad. Esto ayudaría a los usuarios a comprender mejor los derechos y las responsabilidades en la lucha contra el ciberdelito, y promovería una mayor conciencia de los aspectos legales relacionados con esta problemática.

3.4.2.2. Descripción de la aplicación, requisitos técnicos y sus funcionalidades

La aplicación se ha realizado en colaboración con Guillermo Pérez Arias, desarrollador en Telefónica, utilizando lenguaje *Dart*[29] y *Flutter*[30]. La aplicación está disponible para ser descargada y utilizada, aunque todavía no se encuentra en la *PlayStore* o *AppStore*, por lo que para poder utilizarla es preciso solicitar al propietario de la aplicación una versión para su descarga a través de correo electrónico[31].

[29] *Dart* es un lenguaje de fuente abierta desarrollado por Google, que tiene como objetivo permitir a los desarrolladores utilizar lenguajes orientados a objetos con análisis de tipo estático. Desde la primera versión estable en 2011, *Dart* ha cambiado bastante, tanto en el lenguaje como en sus objetivos principales.

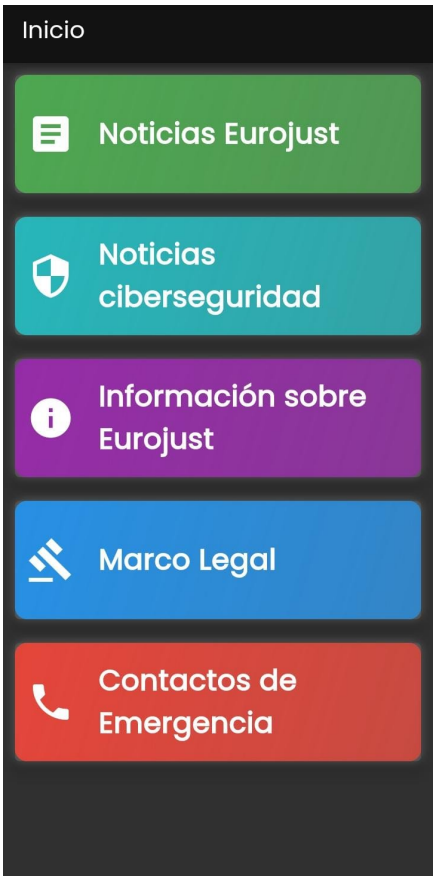
[30] *Flutter* también es un marco de código abierto, desarrollado por Google para crear aplicaciones móviles ya sean Android o iOS.

[31] Para solicitar una copia de la aplicación enviar un email a la siguiente dirección: alejandro.serre@gmail.com

Está organizada en cinco apartados. Cada apartado está compuesto por un modelo de datos (forma que se quiere dar a los datos en la aplicación), un proveedor de servicios (se encarga de consultar la información que provenga de RSS, API u otros archivos, y de transformarla en el modelo de datos definido) y una pantalla (se encarga de consultar el proveedor de servicios y presenta el resultado final que ve el usuario). Podemos visualizar la pantalla de inicio a continuación:

Figura 1

Pantalla de inicio de la aplicación



Nota: la imagen muestra la pantalla de inicio y los cinco apartados que componen la aplicación.

Fuente: imagen tomada de la aplicación móvil desarrollada.

A continuación se procederá a describir las especificaciones técnicas y el contenido de cada uno de los cinco apartados de la aplicación móvil.

- **Apartado de "Noticias Eurojust"**

En este apartado, se encuentran las noticias proporcionadas en la página web oficial de Eurojust. El enlace es el siguiente:
<https://www.eurojust.europa.eu/media-and-events/press-releases-and-news>

Este apartado se ha configurado para que las noticias se encuentren siempre actualizadas, por lo tanto, si una nueva noticia se publica, aparecerá en la aplicación móvil. Para poder configurar este apartado se ha utilizado un servicio RSS[32] (*Really Simple Syndication*). Este recurso se ha utilizado para la distribución de contenidos en tiempo real basado en el lenguaje XML[33].

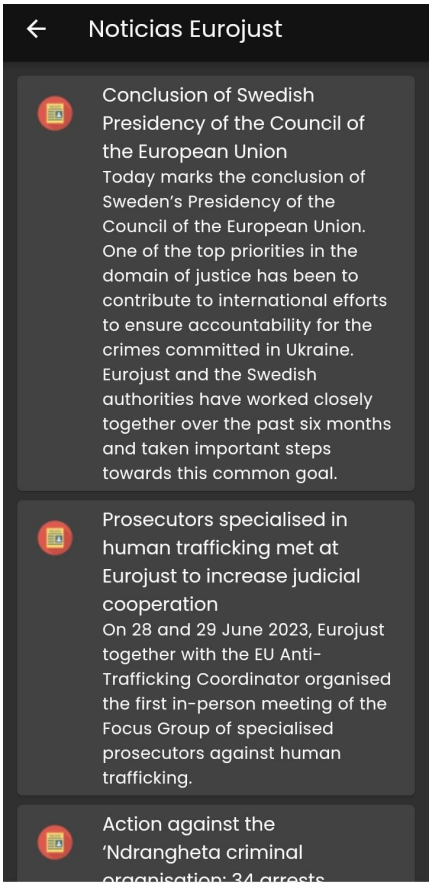
A través de este enlace, que es un archivo XML, se accede y modelan[34] los datos en función de nuestras preferencias: El enlace es el siguiente:
<https://www.eurojust.europa.eu/rss/press-releases.xml>

Las noticias están separadas por tarjetas y al interactuar con cada una de ellas redirigirá al link de la noticia en la página oficial de Eurojust.

[32] Un servicio RSS es una forma de compartir contenido actualizado de una página web a los usuarios que se han suscrito a ella.
[33] XML es un lenguaje de marcado que sirve para almacenar e intercambiar datos de forma estructurada y compartible. Un lenguaje de marcado es un conjunto de símbolos o etiquetas que se usan para definir el contenido y el significado de los datos.
[34] Una vez se consulta el XML, descargamos y convertimos los objetos del xml en objetos en nuestro lenguaje, *Dart*. El servicio se encarga de consultar la web, descarga el xml y transformar ese xml en datos que nos sirvan utilizando el modelo de datos creado "titulo, link y descripción". Por último este proveedor lo consultaremos en la pantalla, y con la información que nos ha convertido este proveedor lo mostraremos visualmente con el formato escogido.

Figura 2

Pantalla de noticias de Eurojust



Nota: la imagen muestra la pantalla del apartado de noticias de Eurojust. Al interactuar con cualquiera de los elementos presentes en este apartado, se nos redirigirá a la noticia y a la página oficial, donde se podrá consultar.
Fuente: imagen tomada de la aplicación móvil desarrollada.

- **Apartado de "Noticias de ciberseguridad"**

Una de las cuestiones que se planteaban en el desarrollo de la aplicación es la dificultad a la hora de encontrar noticias de ciberseguridad en Internet. Si bien es cierto que es un tema de actualidad, poder agrupar todas las noticias relativas a la ciberseguridad era una tarea complicada. Por ello, al considerar esto un aspecto fundamental para cualquier investigador o usuario que quiera estar al tanto de las últimas novedades y actualizaciones, se ha elaborado este apartado.

Estás noticias de ciberseguridad también se encuentran siempre actualizadas. En este apartado, se sigue el mismo patrón que “Noticias de Eurojust”: un modelo de datos, un proveedor de servicios y una pantalla. Una de las grandes diferencias entre este apartado y el de noticias es la utilización de una API[35]. Entre las grandes ventajas de utilizar una API, encontramos que ofrece una mayor personalización y flexibilidad, ya que se puede elegir qué datos o servicios se quieren consumir o proveer.

Además, permite acceder a datos o funcionalidades de otras plataformas o aplicaciones sin tener que conocer su código fuente ni su estructura interna. Sumado a lo anterior también facilita la integración y la interoperabilidad entre diferentes sistemas, lo que mejora la eficiencia y la innovación, y ofrece una mayor personalización y flexibilidad, ya que se puede elegir qué datos o servicios consumir o proveer. Por último, garantiza una mayor seguridad y calidad, ya que los datos o servicios se transmiten mediante protocolos estandarizados y controlados.

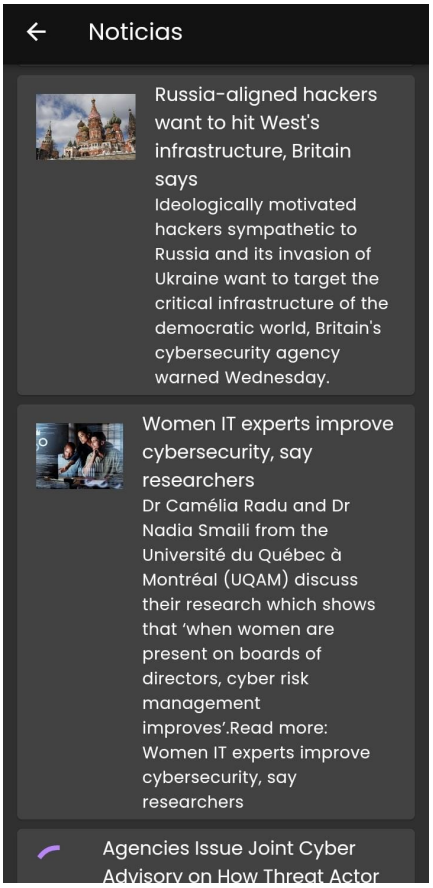
Por lo tanto, la utilización de una API aporta muchas más posibilidades a la hora de consumir datos e información. En este apartado, las noticias también se encuentran separadas por tarjetas, y al interactuar con cada una de ellas, se redirigirá al enlace de la noticia.

Como dato adicional, en caso de que en alguna de las noticias aparezca un círculo de progreso, significa que se está intentando acceder a la imagen pero no está disponible. La aplicación tiene un método para comprobar las imágenes, y para evitar que se produzca un error que resultaría en el cuelgue de la aplicación. No se ha podido utilizar API en el apartado de “Noticias de Eurojust” porque la agencia no dispone de una API.

[35] Un API es una interfaz de programación que permite la comunicación entre diferentes plataformas o aplicaciones en tiempo real.

Figura 3

Pantalla de noticias de ciberseguridad



Nota: la imagen muestra la pantalla del apartado de noticias de ciberseguridad. Al interactuar con cualquiera de los elementos presentes en este apartado, se nos redirigirá a la noticia y a la página oficial donde se podrá consultar.
Fuente: imagen tomada de la aplicación móvil desarrollada.

- **Información sobre Eurojust y marco legal**

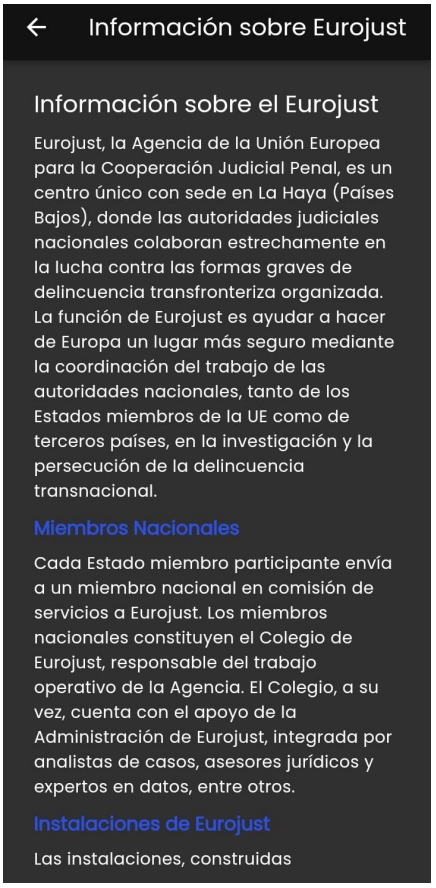
En el tercer y cuarto apartado se utiliza también un modelo de datos, un proveedor de servicios y una pantalla.

En estos dos no se utilizará ni un RSS o API, se utilizan lo denominado como archivos *MarkDown*[36].

[36] *MarkDown* es un documento de texto simple y propio, elaborado de manera personal, lo que permite poner títulos y diversos formatos.

Figura 4

Pantalla de información sobre Eurojust



Nota: la imagen muestra la pantalla del apartado de información sobre Eurojust. Contiene la información básica de la Agencia de la Unión Europea para la Cooperación Judicial Penal.

Fuente: imagen tomada de la aplicación móvil desarrollada.

Figura 5

Pantalla sobre el marco legal de Eurojust

Nota: la imagen muestra la pantalla del apartado de marco legal de Eurojust. Contiene un resumen del Reglamento (UE) 2018/1727 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust), así como los principales tratados y legislación en materia de cibercrimen y cooperación transfronteriza.
Fuente: imagen tomada de la aplicación móvil desarrollada.

- **Contactos de emergencia**

En este apartado hay una lista de los 27 países miembros de la Unión Europea y adicionalmente Reino Unido. Se puede seleccionar cualquiera de los 28 países añadidos en este apartado, y una vez seleccionado se redirigirá a la página web oficial de ciberseguridad de los países. Al redirigir a la página web oficial del país seleccionado, se pretende facilitar el acceso a información relevante sobre la

ciberseguridad en ese país, como contactos de emergencia, recursos, servicios y noticias relacionadas. Esto puede ser útil para obtener información actualizada y confiable sobre ciberseguridad en el país seleccionado.

Los contactos de emergencia mencionados son puntos de referencia importantes en el ámbito de la ciberseguridad. Estos contactos sirven para reportar incidentes de seguridad, recibir asesoramiento, orientación, coordinar respuestas y colaboraciones, intercambiar información relevante, promover la sensibilización y educación en ciberseguridad. Su objetivo principal es garantizar una respuesta rápida y eficaz frente a amenazas cibernéticas, protegiendo los sistemas y datos, y fomentando buenas prácticas en seguridad cibernética tanto a nivel individual como organizacional. Los contactos de emergencia presentes en este apartado son recursos valiosos para abordar los desafíos de la ciberseguridad y fortalecer la protección de la infraestructura digital.

Este apartado se encarga de consultar un archivo elaborado de forma propia y denominado *JSON*[37]. Este archivo se compone de: 1. País 2. Bandera y 3. Agencia de ciberseguridad.

El proveedor se encarga de leer este archivo y la pantalla mostrará la bandera, el país y la agencia, en la que si se clica, se redirigirá a la web correspondiente. También se ha incluido la función de *card swiper* en las tarjetas, lo que permite deslizar y alternar entre las diferentes opciones hasta seleccionar el país deseado.

La aplicación es escalable, es decir, que en caso de necesitar aumentar la funcionalidad (añadir más países, banderas y agencias) se puede realizar de manera sencilla.

[37] *JSON* es un formato de texto sencillo para el intercambio de datos.

Figura 6

Pantalla de contactos de emergencia

Nota: la imagen muestra la pantalla del apartado de contactos de emergencia. Se puede seleccionar el país deseado y visitar el sitio web al interactuar con el recuadro morado.

Fuente: imagen tomada de la aplicación móvil desarrollada.

4. CONCLUSIONES

Los epígrafes anteriores nos han permitido realizar un recorrido completo y examinar el contenido en relación con el papel de Eurojust en la lucha contra el ciberdelito transfronterizo en la Unión Europea, a través del análisis de su marco legal, su eficacia en la cooperación judicial en diversos casos, y las perspectivas de futuro en este tema.

Gracias al estudio y a la investigación exhaustiva que se ha realizado en el presente trabajo, se procederá a formular las siguientes conclusiones de acuerdo con las cinco hipótesis planteadas al comienzo del mismo:

1) El marco legal de Eurojust proporciona el alcance y los mecanismos de cooperación necesarios para hacer frente al cibercrimen transfronterizo.

Según el análisis realizado sobre el marco legal de Eurojust, ya sean los tratados, acuerdos internacionales o legislación de la propia Unión Europea, concretamente el Reglamento sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust), podemos afirmar que el marco legal de Eurojust sí que proporciona el alcance y los mecanismos de cooperación necesarios para hacer frente al cibercrimen transfronterizo.

En primer lugar, se ha podido determinar que las normativas que sustentan la actuación de Eurojust, proporcionan el alcance necesario para poder permitir a dicha agencia y demás autoridades competentes, cooperar de manera eficaz en la lucha del cibercrimen transfronterizo. Prueba de esto se ha podido ver en los numerosos ejemplos que se han expuesto en los diferentes epígrafes del analizado marco legal, como la promoción en la cooperación transfronteriza en la obtención e intercambio de información de pruebas digitales, la armonización de los marcos legales, y los procedimientos de investigación que se realizan entre los Estados miembros de la Unión Europea. Además, ha quedado demostrado que las normativas también

establecen mecanismos de suma importancia para poder hacer frente al cibercrimen transfronterizo, siendo estos los de prevención y disuasión, contribuyendo también a la concienciación y educación en materia de ciberseguridad.

Otro aspecto importante, en relación con los mecanismos de cooperación, es la existencia de los puntos de contacto especializados con los que cuenta cada Estado miembro de la UE. Gracias a esto, la UE se ve beneficiada en aspectos como la comunicación y la coordinación entre las autoridades competentes de cada Estado miembro, para poder hacer frente al cibercrimen transfronterizo. El impacto que los puntos de contacto han tenido en la UE se puede ver traducido en una mayor agilidad y rapidez en el intercambio de información, en las solicitudes de asistencia y en la coordinación de acciones conjuntas para resolver cuestiones de esta índole.

Sumado a lo anterior, es un hecho que las normativas no solo establecen puntos de contacto especializados, sino que también promueven la realización de operaciones conjuntas. Por ello se han establecido Equipos Conjuntos de Investigación (ECIs) para luchar de manera conjunta y coordinada contra el cibercrimen transfronterizo, aumentando la eficacia y contundencia en las investigaciones, mejorando la asignación de recursos, fomentando el uso de herramientas tecnológicas, aprovechando el conocimiento y experiencia de múltiples jurisdicciones, y dotando a las investigaciones de un enfoque integral y multidimensional que resulta clave para abordar estos casos.

2) El marco legal de Eurojust presenta un nivel de especialización insuficiente en la lucha contra el cibercrimen transnacional en comparación con el enfoque específico del Convenio de Budapest.

Para abordar esta cuestión, ha sido realmente importante no solo el estudio del propio Convenio de Budapest sobre ciberdelincuencia, sino la realización de un análisis comparativo entre ambos marcos legales para conocer las similitudes y diferencias en aspectos como el alcance geográfico y jurisdiccional, el enfoque sobre

el ciberdelito, y la cooperación y asistencia legal entre los Estados miembros, a efectos de poder confirmar o desmentir la hipótesis planteada.

Tal y como ha quedado reflejado, el Convenio de Budapest presenta un alcance geográfico y jurisdiccional más amplio, por la gran cantidad de países que pertenecen al convenio. El marco legal de Eurojust le dota de una cooperación internacional en materia de justicia penal mucho más estrecha y flexible. A pesar de ello, el trabajo está centrado específicamente en el cibercrimen, y el Convenio de Budapest ha demostrado tener un enfoque mucho más concreto en este tema, y no tan general como el Reglamento de Eurojust.

Ejemplo de esto es la gran cantidad de artículos y disposiciones presentes en dicho convenio, que han sido elaborados particularmente para afrontar el cibercrimen transfronterizo. El hecho de que el marco legal de Eurojust sea tan general puede crear dificultades y obstáculos a la hora de perseguir los ciberdelitos. Aún así, Eurojust cuenta con una ventaja frente al Convenio de Budapest, siendo esta la calidad y eficacia en la cooperación y asistencia legal entre los Estados miembros, existiendo una mejor orientación y coordinación en investigaciones, medios y recursos.

Dicho lo cual, podemos afirmar que el marco legal de Eurojust presenta un nivel de especialización insuficiente en la lucha contra el cibercrimen transnacional en comparación con el enfoque específico del Convenio de Budapest, aunque la UE presente una mejor cooperación y coordinación. En este sentido, para solucionar este problema, que podría ser considerado como una falta de armonización, se debería plantear la elaboración de un reglamento que contenga disposiciones específicas para abordar el cibercrimen y los ciberdelitos dentro de la Unión Europea, ya que esta cuenta con mecanismos de cooperación y herramientas más que suficientes.

3) Eurojust cuenta con las funciones y competencias necesarias para hacer frente al cibercrimen transfronterizo.

En relación a la tercera hipótesis planteada, podemos afirmar que Eurojust sí que cuenta con las funciones y competencias necesarias para hacer frente al cibercrimen transfronterizo. Esto se debe en primer lugar, al relativamente reciente cambio en las funciones y competencias de Eurojust por la transición de la la Decisión 2002/187/JAI del Consejo al Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, ya que Eurojust fue dotado de mayor libertad e independencia a la hora de actuar. Hay que tener presente, que Eurojust solo podía desempeñar sus funciones previa solicitud expresa de las autoridades nacionales competentes.

Asimismo, el artículo 85.1 del TFUE ha sido clave al describir las funciones de Eurojust, haciendo hincapié en el componente de apoyo y refuerzo en la coordinación y cooperación entre las autoridades nacionales. El Reglamento (UE) 2018/1727 también hace un excelente trabajo en ordenar y desarrollar las competencias y funciones que Eurojust posee, lo que ha sido determinante para que todas las cuestiones operativas cuenten con el respaldo necesario, brindando una mejor asistencia a las autoridades competentes de los Estados, mejorando la coordinación en las investigaciones y análisis realizados, así como el apoyo a los centros de asesoramiento especializados de la UE, y a la acción de los Estados para hacer frente a la ciberdelincuencia, junto con la estrecha cooperación existente con la Fiscalía Europea en asuntos de su propia competencia.

4) Eurojust tiene un impacto limitado en la cooperación judicial internacional, y no ha logrado establecerse como un actor clave y efectivo en la lucha contra el cibercrimen transfronterizo.

Tras el análisis realizado de la eficacia de Eurojust a través el estudio de dos casos emblemáticos, se ha demostrado que Eurojust ha tenido un impacto determinante en la cooperación jurídica internacional, estableciéndose como un actor clave y efectivo

en la lucha contra el cibercrimen transfronterizo, de modo que la hipótesis planteada queda desmentida.

Tal y como se ha mostrado en las dos evaluaciones realizadas sobre los casos *Avalanche* y *Blackshades*, y de acuerdo con los objetivos, criterios y puntuaciones fijados en los epígrafes correspondientes, se puede concluir que el Eurojust ha sido un actor no solo fundamental, sino también efectivo como agencia, al tener un gran impacto en las operaciones en las que participa, y por ende contribuyendo a la lucha contra el crimen transfronterizo. La agencia ha conseguido liderar, coordinar y apoyar investigaciones conjuntas, organizar reuniones y facilitar el intercambio rápido de información para resolver los casos.

5) La adopción de nuevas tecnologías y enfoques innovadores son necesarios para que Eurojust mejore la eficiencia y la eficacia de la cooperación jurídica internacional en los desafíos actuales y futuros.

La quinta y última hipótesis planteada en el presente trabajo de investigación queda confirmada, ya que gracias al análisis de los desafíos actuales y futuros en la cooperación jurídica internacional en la UE, tales como la geometría variable, la ejecución de solicitudes de asistencia legal mutua, y la importancia de las redes sociales para aplicaciones como *Big data*, se ha podido concluir que la UE necesitará desarrollar y aplicar enfoques innovadores, para la elaboración de nuevas herramientas legales, que sean flexibles y que contribuyan a una cooperación jurídica internacional de mayor calidad y eficacia, a través del uso de las nuevas tecnologías.

Para ello se ha desarrollado una aplicación móvil, para proporcionar a los usuarios una herramienta que sea accesible y práctica a la hora de consultar la información relevante y actualizada sobre Eurojust, y las noticias que atañen a la agencia, así como crear un medio que permita acceder rápidamente a los recursos necesarios, en caso de ser víctimas de un ciberataque o presenciar actividades delictivas en línea.

5. FUENTES NORMATIVAS

Instrumento de ratificación de la Convención de las Naciones Unidas contra la corrupción, hecha en Nueva York el 31 de octubre de 2003. *Boletín Oficial del Estado núm. 171* del 19 de julio de 2006. https://www.boe.es/eli/es/ai/2003/10/31/(1)

Instrumento de Ratificación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Nueva York el 15 de noviembre de 2000. *Boletín Oficial del Estado núm. 233* del 29 de septiembre de 2003. https://www.boe.es/eli/es/ai/2000/11/15/(1)

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. *Boletín Oficial del Estado núm. 226* de 17 de septiembre de 2010.https://www.boe.es/eli/es/ai/2001/11/23/(1)

Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo, 295 OJ L (2018). *Diario Oficial de la Unión Europea*. http://data.europa.eu/eli/reg/2018/1727/oj/spa

6. BIBLIOGRAFÍA

Abreu Valencia, F. A. (2022). La cooperación internacional en materia de cibercrimen y evidencia digital. *Saber y Justicia*, *1*(21), 30-53. https://dialnet.unirioja.es/servlet/articulo?codigo=8500602

Alonso Moreda, N. (2012). Eurojust, a la vanguardia de la cooperación judicial en materia penal en la Unión Europea. *Revista de Derecho Comunitario Europeo*, *16*(41), 119-157. https://dialnet.unirioja.es/servlet/articulo?codigo=4019204

Alonso Salgado, C. (2019). Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo. *Ars Iuris Salmanticensis: AIS : revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, *7*(1), 325-326. https://dialnet.unirioja.es/servlet/articulo?codigo=7166787

Aurestic. (2022). *¿Qué es Flutter? - Desarrollo de Aplicaciones móviles | Aures Tic*. https://aurestic.es/que-es-flutter/

Bejarano, M. J. C. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Instituto Español de Estudios Estratégicos*, 47-82.

Bermudez, J. D., Castro, J. J., Peralta, A., & Guacaneme, P. A. (2023). *Técnicas Avanzadas de Ciberseguridad: Integración y Evolución de la Kill Chain en Diversos Escenarios*.

Brière, C. (2018). *Cooperation of Europol and Eurojust with External Partners in the*

Fight Against Crime: What are the Challenges Ahead? https://dcubrexitinstitute.eu/wp-content/uploads/2018/01/WP-2018-1-Bri%C3%A8re.pdf

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, *8*, Article 8. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321

Escalada López, M. L. (2023). La Cooperación judicial en la UE. Especial referencia a Eurojust y a las novedades normativas que le afectan. *Revista de Estudios Europeos*, *Extraordinario monográfico 1*, Article Extraordinario monográfico 1. https://doi.org/10.24197/ree.Extraordinario

European Union Agency for Criminal Justice Cooperation. (2015). *Operation Blackshades: An evaluation*. https://www.eurojust.europa.eu/publication/operation-blackshades-evaluation

European Union Agency for Criminal Justice Cooperation. (2017). *Operation Avalanche: A closer look.* https://www.eurojust.europa.eu/publication/operation-avalanche-closer-look

European Union Agency for Criminal Justice Cooperation. (2020). *Challenges and best practices from Eurojust's casework in the area of cybercrime*. https://www.eurojust.europa.eu/publication/challenges-and-best-practices-eurojusts-casework-area-cybercrime

Fojón Chamorro, E., & F. Sanz Villalba, Á. (2010). Ciberseguridad en España: Una propuesta para su gestión. *Real Instituto Elcano*.

https://www.files.ethz.ch/isn/118153/ARI102-2010_Fojon_Sanz_ciberseguridad_Espana.pdf

Hernández López, A. (2020). El Reglamento (UE) 2018/1727 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust): Luces y sombras al amparo de los arts. 85 y 86 TFU. *Revista de estudios europeos*, *75 (Enero-Junio)*, 225-241. https://dialnet.unirioja.es/servlet/articulo?codigo=7216852

Inlab FIB. (2020, mayo 26). *¿Qué es el lenguaje de programación Dart?* inLab FIB. https://inlab.fib.upc.edu/es/blog/que-es-el-lenguaje-de-programacion-dart

Newmeyer, K. (2015). Ciberespacio, ciberseguridad y ciberguerra. *Escuela Superior de Guerra Naval*.

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. *Cooperativa Cyber Defence Centre of Excellence*. https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf

Pérez Souto, G. (2013). Eurojust: ¿un instrumento eficaz en la lucha contra el crimen organizado? *Revista General de Derecho Europeo*, *30*, 4. https://dialnet.unirioja.es/servlet/articulo?codigo=4508930

Prado, A. F. R. (2022). *El cibercrimen en Colombia y su evolución en los últimos dos años (2020-2021)*.

Proofpoint. (2021, junio 13). *¿Qué es un ataque DDoS? - Significado y tipos | Proofpoint ES*. Proofpoint. https://www.proofpoint.com/es/threat-reference/ddos

Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen:

Particularidades en su investigación y enjuiciamiento. *Anuario jurídico y económico escurialense*, 209-234.

Torres Pérez, M. (2022). Eurojust, veinte años de compromiso por la cooperación judicial penal en Europa. El futuro de la Agencia ante la guerra en Ucrania. *Revista electrónica de estudios internacionales (REEI)*, *44*, 7. https://dialnet.unirioja.es/servlet/articulo?codigo=8783258

Valdez Alvarado, A. R. (2012). El cibercrimen. *IUS Ediciones*. https://d1wqtxts1xzle7.cloudfront.net/55996005/articulo_CIBERCRIMEN-libre.pdf?1520473094=&response-content-disposition=inline%3B+filename%3DEl_Cibercrimen.pdf&Expires=1687979427&Signature=dX1n-MX8GlNa6hkdkQe8NObFkdVWLF259RLqPhtrmmhYwOQJGZAftmW6LcNnSCyd10ijM~VQp2~4N-uSkfFsXGRm7XwBWPicyMf0pwIMITwThjcYN2fxqSabWd-~8HO-airQ98lgjpRGcTBzcm0Mxf~Tgjc1CRYrlfWCUnYUhbLO61WhASFQFsIms4a~wddkNFJ4f~LcMV0N~ykqKemBdPuaYV4ehfYB~TvyshWw~6RgmJB7CG~5gil6D7sPK39du7kjIrvRE5vns3Q~rfJIcMR0DELFKPRBvZT88ECr7VEN9CFuLwTX9P-dv1AhZzo3rnPMIpVa32ynzZu6yY463w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Wainwright, R., & Cilluffo, F. J. (2017). *Responding to Cybercrime at Scale: Operation Avalanche — A Case Study*. Center for Cyber and Homeland Security at Auburn University. https://www.jstor.org/stable/resrep20752