FACULTAD DE DERECHO

COOPERACIÓN ENTRE LA INTERPOL Y NACIONES UNIDAS ANTE EL INCREMENTO DE LA CIBERDELINCUENCIA

Autor: Gadea Saldaña López

4º E-1

Derecho Internacional Público

Tutor: Antonio Díaz Narváez

Madrid

2025

ÍNDICE

Resumen

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) ha generado un gran cambio en el estilo de vida de la mayoría de las personas alrededor del mundo. Esta evolución se ha producido en todos los ámbitos, alcanzando el área de este trabajo, la delincuencia.

Las nuevas tecnologías nos ofrecen infinidad de mejoras y ventajas para nuestro día a día a nivel personal, familiar, laboral y educativo. El problema llega en el momento en el que dichas ventajas pasan a ser utilizadas con ánimo delictivo, con la finalidad de obstruir, adquirir o modificar la seguridad digital, lo que se ha venido a denominar "Ciberdelincuencia".

Los delitos informáticos han pasado a constituir una amenaza global tanto para las personas físicas como jurídicas, entes gubernamentales y organismos internacionales ya que, la ciberdelincuencia, no entiende de barreras físicas ni geográficas.

Teniendo en cuenta este marco general, el presente trabajo se centra, en primer lugar, en estudiar la ciberdelincuencia, su naturaleza, modalidades y su impacto global tanto a nivel interpersonal como institucional. A continuación, y para profundizar en materias de Derecho Internacional Público, que es en la rama del Derecho sobre la que se estructura este trabajo, se analizarán las principales medidas, regulaciones, políticas y operaciones de la INTERPOL y de Naciones Unidas en su lucha contra las amenazas que provienen de este tipo de delincuencia, así como la eficacia de las mismas en un mundo digital en constante evolución.

Palabras clave: TIC, Ciberdelincuencia, INTERPOL, Naciones Unidas, delitos informáticos, Ciberespacio.

Abstract

The development of Information and Communication Technologies (ICT) has brought about a major change in the lifestyle of most people around the world. This evolution has taken place in all areas, reaching the area of this work, crime.

New technologies offer us an infinite number of improvements and advantages for our daily lives, at a personal, family, work, and educational level. The problem comes when

these advantages are used for criminal purposes, with the aim of obstructing, acquiring or modifying digital security, which has come to be known as 'cybercrime'.

Cybercrime has become a global threat to natural and legal people, governmental bodies and international organizations, as cybercrime knows no physical or geographical barriers.

With this general framework in mind, this paper focuses firstly on the study of cybercrime, its nature, its modalities, and its global impact on both interpersonal and institutional levels. Next, and in order to delve deeper into matters of Public International Law, which is the branch of law on which this work is based, we will analyze the measures, regulations, policies and operations of INTERPOL and the United Nations in their fight against the threats arising from this type of crime, as well as their effectiveness in a constantly evolving digital world.

Keywords: ICT, cybercrime, INTERPOL, United Nations, cybercrime, cyberspace.

1. Introducción

Durante los últimos años, las Tecnologías de la Información y la Comunicación (en adelante, TIC) han evolucionado de manera exponencial transformando nuestro día a día, rompiendo barreras geográficas, aumentando la productividad laboral, creando diferentes formas de aprendizaje y ofreciéndonos infinidad de entretenimientos. Sin embargo, esta rápida y reciente incorporación de los avances tecnológicos a nuestra vida cotidiana también tiene su lado negativo.

Todas las actividades anteriormente descritas pueden realizarse a través de medios informáticos debido a la gran variedad de datos que éstos recopilan cuando se hace uso de ellos. De hecho, la forma más común de acceder a nuestra información se produce en el momento en el que se acepta el tratamiento de éstos tal y como se recogen en los términos de uso y condiciones que aparecen en el momento en el que se comienza a utilizar un servicio electrónico, una página web o una aplicación específica ("*App"*[1]).

Otra forma de recopilar información se lleva a cabo a través de las denominadas *"cookies"* que, como define la Real Academia Española, *"(...) son pequeños ficheros que*

[1] Según la Real Academia de la Lengua Española (RAE), la palabra "aplicación" hace referencia a: "*Programa informático preparado para una utilización específica, como la contabilidad, el uso de determinadas bases de datos, utilización de juegos, llevanza de películas, audiciones musicales, etc".*

se instalan en el disco duro o en el navegador del ordenador, tableta, teléfono inteligente o dispositivo equivalente con funciones de navegación a través de Internet y ayudan, entre otras cosas, a personalizar los servicios del titular de la web, facilitar la navegación y usabilidad a través de ella, obtener información agregada de los visitantes de la web, posibilitar la reproducción y visualización de contenido multimedia en la propia web, permitir elementos de interactuación entre el usuario y la web o habilitar herramientas de seguridad"[2] .

La confianza con la que utilizamos los medios electrónicos hace posible el almacenamiento de multitud de datos y, con ello, la aparición de diversas modalidades delictivas que se han ido desarrollando exclusivamente en el ámbito digital. Este tipo de delincuencia se denomina ciberdelincuencia y se refiere a todas las actividades delictivas que se llevan a cabo a través de medios informáticos aprovechando el gran uso que hacemos de los mismos y que se diversifica y desarrolla en paralelo al de las tecnologías.

La ausencia de límites geográficos, así como la lentitud de la legislación en tipificar y regular este tipo de delitos han convertido a la ciberdelincuencia en un problema global. Estas actividades delictivas no se suelen limitar únicamente al robo de información a individuos, sino que su espectro se ha ido ampliando hasta el punto de incluir ciberataques a empresas y gobiernos, lo que pone en riesgo una serie de factores globales de índole económico y geopolítico que afectan a la privacidad y la seguridad de los ciudadanos, los entes empresariales y las instituciones internacionales. Ante estos desafíos, algunos organismos internacionales han tomado una posición significativa a nivel mundial mediante la creación de iniciativas para la lucha contra la ciberdelincuencia.

1.1. Justificación del estudio

En un mundo cada vez más interconectado, la ciberdelincuencia se ha transformado en una de las amenazas más importantes para la seguridad mundial que afecta a gobiernos, empresas y ciudadanos.

El progreso tecnológico y la rápida digitalización de los servicios han incrementado los crímenes cibernéticos que abarcan, desde el hurto de información y la estafa en línea, hasta los ataques a infraestructuras críticas. Esto no solo supone un reto técnico, sino también, una cuestión de seguridad global que requiere una reacción coordinada a nivel

[2] *Ibid.:* Real Academia Española. *Política de cookies*. Real Academia Española (s.f.) (disponible en https://www.rae.es/politica-de-cookies; última consulta 25/02/2025).

internacional a través de la armonización legislativa en la materia y de la creación de instituciones de carácter internacional dedicadas a la lucha contra la ciberdelincuencia.

El tema elegido para el presente trabajo viene motivado por la necesidad de examinar esta nueva corriente delictiva y analizar cómo dos de las organizaciones internacionales más importantes del mundo, la Organización Internacional de Policía Criminal (en adelante, INTERPOL) y la Organización de las Naciones Unidas (en adelante, ONU), colaboran para paliar estas amenazas. Estas entidades juegan un papel de especial relevancia en la lucha contra la ciberdelincuencia. De ahí que, el objeto de este estudio sea investigar su organización y armonización para desarrollar una estrategia mundial más eficaz en la lucha contra la ciberdelincuencia.

A pesar de que existen estudios sobre la ciberdelincuencia y las medidas que han adoptado dichas entidades en su lucha contra la misma, en la actualidad son escasos los estudios que analizan cómo la INTERPOL y la ONU pueden avanzar en el combate contra esta, la salvaguarda de los derechos humanos y la reducción de las amenazas digitales a través de una armonización legislativa. Este análisis, por lo tanto, busca cubrir dicho espacio y aportar al debate académico sugerencias y propuestas para potenciar la colaboración internacional entre ambos organismos para reducir la ciberdelincuencia.

1.2. Objetivos del trabajo

El propósito de este trabajo de investigación es analizar el impacto global de los delitos informáticos a raíz del avance de las nuevas tecnologías que se llevará a cabo mediante lo siguiente:

- Delimitar el concepto de ciberdelincuencia y sus modalidades.
- Realizar un estudio de las políticas desarrolladas por la INTERPOL y Naciones Unidas, de las aprobadas y de las que están en proceso, para determinar su impacto en la lucha contra los delitos informáticos.

Lo anterior permitirá justificar las conclusiones que se alcancen en el presente trabajo acerca de la eficacia de la ciberseguridad, su situación global actual, sus principales y la normativa intergubernamental implementada por dichos organismos.

Asimismo, el presente trabajo persigue dar una valoración de la eficacia de la normativa actual y ofrecer una serie de alternativas que permitan combatir de una manera más eficiente mediante la cooperación internacional la situación criminal en el mundo digital.

1.3. Metodología

Para el desarrollo de este trabajo de investigación, la metodología utilizada ha sido de carácter cualitativo y documental, basada en el análisis de diversas fuentes jurídicas y doctrinales con el objetivo de ofrecer una visión completa de la temática del trabajo. Con esto, se busca analizar su aplicabilidad a situaciones reales, comprobando su eficacia y efectuando comparaciones entre diversas normativas sobre la materia con la finalidad de identificar posibles mejoras mediante la interpretación hermenéutica de los diferentes textos legales.

En primer lugar, se ha hecho uso de varias fuentes digitales de carácter oficial, incluyendo páginas web de organismos internacionales como Naciones Unidas e INTERPOL. Esto ha proporcionado información actualizada sobre la normativa vigente y la que está pendiente de aprobación, así como informes y comunicados oficiales que han sido de utilidad para el análisis jurídico de la situación.

Además, se han utilizado diversos artículos académicos y trabajos de investigación realizados sobre la materia, ayudando a formar una opinión crítica de la situación global de la ciberdelincuencia.

También se ha realizado un análisis de la normativa internacional vigente en materia de ciberdelincuencia, así como aquella que se encuentra en vías de aprobación. Esto comprende reglamentos, convenciones y tratados internacionales cuyo objetivo es crear un espacio digital más seguro a nivel global mediante la cooperación intergubernamental.

Finalmente, en orden a valorar la eficacia de la normativa en la práctica, se han analizado operaciones reales contra la delincuencia digital llevado a cabo por la INTERPOL y Naciones Unidad. Todo esto con el propósito de analizar la eficacia de las diferentes regulaciones, así como una valoración de su impacto y posibles vías de desarrollo.

Tanto el material utilizado como la metodología para la realización del trabajo ha sido fundamental para la creación de un estudio estructurado y fundamentado que se basa en un amplio estudio jurídico de la situación internacional de la ciberdelincuencia y su impacto.

1.4. Estructura del trabajo

Este trabajo se ha organizado teniendo como eje principal el estudio de la cooperación entre INTERPOL y las Naciones Unidas en la lucha contra la ciberdelincuencia.

En primer lugar, se ha realizado una delimitación del término "ciberdelincuencia", analizando el impacto actual de la misma, así como su proyección a futuro. Con este análisis se pretende sentar las bases que permitan comprender la magnitud de esta materia y la envergadura del reto al que se enfrentan las entidades internacionales.

Posteriormente, se abordará el estudio del Convenio de Budapest, como principal instrumento de cooperación internacional y armonización legislativa para la lucha frente a la ciberdelincuencia. En este sentido, se analizará su estructura y contenido, así como los protocolos complementarios, lo que permitirá comprenderlas primeras iniciativas tomadas para regular los crímenes cibernéticos y sus modalidades a escala mundial.

A continuación, se llevará a cabo un análisis de la INTERPOL. Mediante el estudio de la organización, sus áreas y programas especializados en este tipo de delitos, se busca conocer su marco normativo interno y su aplicación a operaciones para luchar contra la ciberdelincuencia. En este sentido, se revisarán tanto el Estatuto de la INTERPOL como su Reglamento sobre el tratamiento de datos, lo que permitirá exponer las medidas establecidas para una efectiva cooperación internacional.

En el apartado Quinto del documento se expone la estructura, normativa y operaciones de la ONU en el ámbito de la lucha contra la ciberdelincuencia. En este apartado se hace referencia a la Oficina de Lucha contra el Terrorismo (OLCT), departamento de la organización encargado de las operaciones relacionadas con la delincuencia en el ciberespacio, y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). Se analizará también la Convención de Naciones Unidas en materia de ciberdelincuencia, de cara a subrayar todas aquellas medidas de cooperación y trabajo con otros estados ante la situación actual.

En el apartado Sexto, y una vez analizados los elementos más relevantes en materia de ciberdelincuencia de ambos organismos, se procede a analizar, la cooperación entre la INTERPOL y la ONU. En esta línea, se exponen las medidas de colaboración existentes y los casos de éxito llevados a cabo entre ambas instituciones. Por otro lado, también se tendrán en cuenta los obstáculos existentes en este ámbito, los mecanismos de armonización normativa y la importancia de la protección de los derechos humanos en el ciberespacio. Tomando como base lo anterior, se realizará una identificación fundamentada del panorama mundial actual y de las posibles amenazas y debilidades

encontradas en el mismo, lo que permitirá proponer soluciones de colaboración internacional que no se han tenido en cuenta hasta el momento.

Lo anterior permitirá entender cuál es la situación actual de los delitos cibernéticos y, qué medidas se están tomando para combatirlos por parte de las principales organizaciones internacionales en materia de seguridad

Por último, el apartado de conclusiones recoge una reflexión sobre las amenazas y desafíos identificados, así como las posibles soluciones y oportunidades futuras.

2. La ciberdelincuencia

2.1. Definición de ciberdelincuencia

El nacimiento de internet en el siglo XX ha traído consigo la revolución la sociedad mediante la modificación de sus hábitos y estilo de vida. Estos cambios provocados por la adopción de tecnologías emergentes en nuestro día a día. Han revolucionado el mundo empresarial, educativo y las relaciones personales, generando un entorno más interconectado a nivel global, lo que también implica nuevas amenazas para la seguridad de los datos tanto de personas físicas como de entidades empresariales y gubernamentales.

Este auge de las TIC ha venido acompañado de la creación de nuevos comportamientos delictivos que se enmarcan en lo que ha venido a denominarse como "ciberdelincuencia".

La reciente resolución número 79/460 del 27 de noviembre de 2024[3] aprobada por la Asamblea General de Naciones Unidas en relación con la Convención de Naciones Unidas contra la Ciberdelincuencia, define las TIC en su artículo 2 como *"todo dispositivo o conjunto de dispositivos interconectados o relacionados entre sí cuya función, o la de alguno de sus elementos, sea reunir, almacenar y procesar automáticamente datos electrónicos mediante la ejecución de un programa"*[4].

Desde la ONU se apoya la idea de que estos avances puedan fomentar el desarrollo de los 17 Objetivos de Desarrollo Sostenible (en adelante, ODS), constituyendo el acceso a las

[3] Organización de las Naciones Unidas (ONU). (2024). *Informe del Secretario General sobre la labor de la Organización*, A/79/460 (disponible en https://docs.un.org/es/A/79/460; última consulta en 20/03/2025).
[4] En términos similares, una definición amplia de lo que se consideran las TIC es aquella realizada por la empresa española multinacional Telefónica S.A., la cual lo describe como "*todas aquellas infraestructuras y herramientas que permiten tanto la conexión entre personas como la recogida y análisis de información". Vid.:* https://www.telefonica.com/es/sala-comunicacion/blog/que-son-las-tic-y-para-que-sirven/

tecnologías de la información y la comunicación como uno de los retos incluidos en la Agenda 2030 (Pacto Mundial de la ONU España, 2023)[5].

La ciberdelincuencia[6] es un delito que, debido a la evolución de las nuevas tecnologías, ha crecido notablemente a nivel mundial. Este nuevo delito puede tipificarse en el ataque a sistemas, redes o sitios web, entre otros, haciendo uso de la red y las nuevas tecnologías, con la intención de comprometer la seguridad de la información de los usuarios, infringiendo así la normativa establecida y vulnerando los derechos personales.

El "*Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia"*[7] en su artículo 2.1 define ciberdelincuencia como *"cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación"*[8]. Este tipo de delitos han sido descritos por la Oficina de las Naciones Unidas contra la Droga y el Delito (en adelante, UNODC), como aquellos que no tienen *"barreras físicas ni geográficas" (Oficina de las Naciones Unidas contra la Droga y el Delito, s.f.)*[9].

La UNODC, considera la ciberdelincuencia como un crimen de amenaza global por la ausencia de fronteras, que puede ser cometido por cualquier persona, en cualquier región, contra víctimas que pueden ser tanto personas físicas como jurídicas, estados u organizaciones, siendo cada vez mucho más sofisticados los medios y la forma de actuar de los cibercriminales, lo que incrementa la complejidad para identificar al culpable. Estos tipos de ataques vulneran lo conocido como la *"Triada CIA" (TechTarget, s.f.)*[10],

---

[5] Pacto Mundial de la ONU España. "*Potencialidades y debilidades del sector de las TIC ante los ODS"*. *Pacto* Mundial. 5 de diciembre de 2023 (disponible en https://www.pactomundial.org/noticia/potencialidades-y-debilidades-del-sector-de-las-tics-ante-los-ods/; última consulta 27/03/2025).

[6] *Vid.:* Centro de Formación de la Cooperación Española. (2021). La ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional (segunda edición), 2021 (disponible en https://goo.su/U2Ic1M4; última consulta en 30/03/2025).

[7] *Vid.:* Consejo de los Ministerios de Justicia de los Países Iberoamericanos (COMJIB). "*Entra en vigor el Convenio Iberoamericano de Cooperación en materia de Ciberdelincuencia"*, 17 de julio de 2023 (disponible en https://comjib.org/entra-en-vigor-el-convenio-iberoamericano-de-cooperacion-en-materia-de-ciberdelincuencia/; última consulta 27/03/2025).

[8] Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia. (28 de mayo de 2014)

[9] Oficina de las Naciones Unidas contra la Droga y el Delito. "*Cybercrime in brief"*, UNODC, (s.f.) (disponible en https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html; última consulta 20/03/2025).

[10] *Cfr.:* TechTarget. "*Confidentiality, integrity and availability (CIA)"*, TechTarget, (s.f.) (disponible en https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA; última consulta 27/03/2025).

cuyas siglas hacen referencia a la Confidencialidad, la Integridad y la Accesibilidad de los sistemas informáticos que se han visto vulnerados. Este concepto nace como herramienta para la creación e implementación de políticas de seguridad en el ámbito de la regulación de la información que contienen las diferentes organizaciones.

En primer lugar, la confidencialidad se basa en las medidas que se deberán de adoptar para salvaguardar los datos privados de los usuarios o miembros de la organización que hayan visto vulnerada su intimidad debido al acceso de terceros no autorizados. Para su correcta regulación la información se clasifica en función del impacto negativo que podrían generar a su propietario en el caso de caer en las manos incorrectas.

Seguidamente, la nota de integridad hace referencia a la conservación de los datos iniciales y, por lo tanto, a la implementación de medidas para que estos no sean manipulados por una tercera persona como, por ejemplo, a través de la incorporación de políticas de acceso a sistemas o el requerimiento de firmas digitales.

Por último, la accesibilidad se refiere a la disponibilidad de la información mediante el cuidado e incorporación de sistemas de datos fiables que permitan la actualización de los datos y su accesibilidad para todo aquel que esté habilitado a ello. En esta nota se aboga por la toma de decisiones en orden a conseguir políticas y medidas paro casos relacionados con la pérdida o manipulación de datos[11].

Como dijo el expresidente de la INTERPOL Meng Hongwei en la 86ª reunión de la Asamblea General de la organización en el año 2017, *"Cada año se cometen 170 millones de ciberdelitos, que causan unas pérdidas estimadas en 445 000 millones de USD, y, sin embargo, solo se resuelve un caso de cada mil. Y todo esto solo es el principio"*[12].

[11] *Vid.:* Universidad Internacional de La Rioja (UNIR). *"Principios de seguridad informática*", UNIR Revista. (s.f.). (disponible en https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/; última consulta 27/03/2025).

[12] Meng, H. "*Ir con los tiempos y mantener las esperanzas de un siglo - Una INTERPOL que mira al futuro"*. Discurso presentado en la 86ª reunión de la Asamblea General de INTERPOL, Beijing, China. 26 de septiembre de 2016 (disponible en https://www.interpol.int/es/content/download/5351/file/17Y1721%20S%20DISCURSO%20PRESIDENTE%2086%20REUNION%20AG.pdf; última consulta 27/03/2025).

2.2. Tipos

El Convenio de Budapest sobre la Ciberdelincuencia del año 2001 (en adelante, el Convenio)[13], impulsado por el Consejo de Europa constituyéndose como el primer texto internacional en esta materia, reconoce e implementa medidas relativas a la cooperación entre los Estados contra las amenazas surgidas a raíz de la evolución de las tecnologías[14].

El Convenio diferencia dentro de su capítulo II titulado, "Medidas que deberán de adoptarse a nivel nacional", los siguientes tipos de delitos:

I. *"Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*": los artículos del 2 a 6 del Convenio recogen la necesidad de que los estados miembros adopten medidas en relación con el acceso, la obstrucción, modificación, uso y apropiación deliberada e ilícita de datos y dispositivos, medios o programas informáticos.

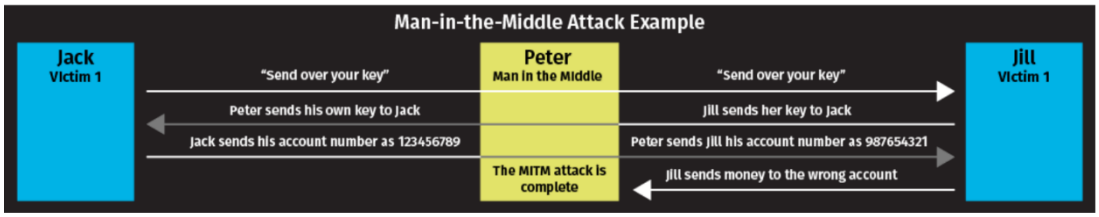
   Dentro de este tipo de delitos se encuentran las acciones dirigidas contra páginas web, la piratería informática y la creación de softwares maliciosos (*malware*).

   Este último término hace referencia al acceso ilícito e intencional a sistemas de información para los que no se está autorizado, comprometiendo la seguridad de la información confidencial de los usuarios de las diferentes redes. La creación de este tipo de *malware* tiene como finalidad la monitorización de sistemas de información mediante la incorporación de *softwares* maliciosos con la intención de modificar, dañar o adquirir datos.

   Como ejemplo de este tipo de delitos nos encontramos con el denominado *"Man in the middle"* (MITM)[15]. Este supone una amenaza contra la seguridad en línea de los usuarios basada en un ataque a través de la interceptación de las comunicaciones entre el usuario y los servidores de manera que, al ser los delincuentes los intermediarios, tiene el acceso a toda la información entre las partes. El objetivo que se persigue consiste en recibir, acceder o enviar información mediante la creación de conexiones ilícitas.

---

[13] *Vid.: "El Convenio de Budapest sobre la Ciberdelincuencia: importancia, beneficios y sus protocolos adicionales",* 23 de noviembre de 2001, apartado 3, P. 19.
[14] *Vid.:* Apartado 3, P. 20 de este trabajo.
[15] *Vid.:* Código de Vera. "*Ataque de intermediario (MITM)"*. Código de Vera, s. f. (disponible en https://www.veracode.com/security/man-middle-attack/; última consulta 20/03/2025).



(Veracode, s.f.)

II. *Delitos informáticos:* los artículos 7 y 8 del Convenio hacen referencia a las medidas que deberán tomar las partes en relación con la modificación, incorporación, la interferencia o la eliminación de datos. Mediante estas acciones, los ciberdelincuentes generan una información falsa tipificándose esto como un delito en el caso de cometerse de manera dolosa con fines ilícitos, ya que generan perjuicios personales y/o patrimoniales a los usuarios.

El Convenio sobre delitos cibernéticos del Consejo de Europa establece en su artículo 5 la definición de *"interferencia del sistema*". Con este concepto hace referencia al *"obstáculo grave intencional e ilegítimo del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, eliminación, deterioro, alteración o supresión de datos informáticos".*

Dentro de esta categoría, el Proyecto de estudio exhaustivo sobre los delitos cibernéticos de la UNODC del año 2013[16], incorporó como tipo de actividad delictiva el fraude o la falsificación informática, delitos contra la identidad, el envío o control de spam, acciones contra la propiedad intelectual y el llamado *"grooming"*[17].

La falsificación informática, hace referencia a las suplantaciones de identidad en línea con el objetivo de conseguir información o transferencias económicas. Dentro de estos se encuentra el "*phishing"*[18], el cual se produce a través del envío de correos o mensajes falsos, con el objetivo de engañar al receptor para que realice una serie de acciones deseadas por el atacante y dirigidas a conseguir información sensible del receptor.

---

[16] *Cfr.:* Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). "*Estudio exhaustivo sobre el delito cibernético".* Naciones Unidas, 2013. (disponible en https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf; última consulta 27/03/2025).

[17] *Vid.:* Save the Children España. "*Grooming: Qué es, cómo detectarlo y prevenirlo".* Save the Children España, s.f. (disponible en https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo; última consulta 27/03/2025).

[18] *Vid.:* IBM. "*Suplantación de identidad (phishing)*(sf). *Phishing".* IBM, s.f. (disponible en https://www.ibm.com/es-es/topics/phishing; 27/03/2025).

III. El artículo 9 del Convenio se refiere a aquellos actos cuya finalidad sea producir, obtener y/o difundir material pornográfico de carácter infantil.

Ante estas amenazas, la Organización Internacional de Policía Criminal (INTERPOL) y el Fondo de las Naciones Unidas para la Infancia (UNICEF)[19] firmaron un acuerdo con el objetivo de colaborar ante la investigación de los delitos contra menores. El acuerdo establece los papeles que adoptarán ambas organizaciones para con los grupos nacionales especializados en orden a ofrecer protocolos más eficaces y rápidos mediante el fomento de creación de grupos de investigación, formaciones y sistemas informáticos especializados en la materia. En este sentido Catherine Russell, Directora Ejecutiva de UNICEF señaló que *"La explotación y el abuso sexual de menores son una lacra mundial. La colaboración intersectorial y transfronteriza es fundamental para hacer frente a este problema"*[20].

IV. Por último, el artículo 10 del Convenio recoge, los "*delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines".*

De los delitos antes indicados, el *phishing* y el *ransomware*[21], son los más utilizados, ya que, a través de la instalación de *malwares*, persiguen la captación de información confidencial de los usuarios.

En particular, el *phishing* tiene como objetivo la suplantación de la identidad de los usuarios a través del envío de mensajes, enlaces o archivos fraudulentos vía correo electrónico, y ha evolucionado hacia nuevas formas delictivas como el *pharming*, el cual se dedica a redirigir a los usuarios a páginas web infectadas o fraudulentas para sustraer información confidencial.

El *ransomware*[22] constituye una de las principales preocupaciones a nivel global. A través de este tipo delictivo, los atacantes tienen como finalidad la obtención de información

---

[19] *Vid:* UNICEF. "*¿Qué hacemos?"* Unicef, s.f. (disponible en https://www.unicef.org/es/que-hacemos, último acceso 27/03/2025).

[20] *Vid.:* INTERPOL. "Yo*INTERPOL y UNICEF firman un acuerdo de cooperación para combatir la explotación y el abuso sexual de menores", 2023. (disponible en* https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2023/INTERPOL-y-UNICEF-firman-un-acuerdo-de-cooperacion-para-combatir-la-explotacion-y-el-abuso-sexual-de-menores; última consulta en 27/03/2025).

[21] *Vid.:* INTERPOL. "*Urge actuar de inmediato para evitar una pandemia de ransomware",* INTERPOL., 2021 (disponible en https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/Urge-actuar-de-inmediato-para-evitar-una-pandemia-de-ransomware-INTERPOL; última consulta en 27/03/2025).

[22] *Vid.:* IBM. "*Ransomware"*. IBM, s.f. (disponible en https://www.ibm.com/es-es/topics/ransomware; última consulta en 27/03/2025).

confidencial o programas de las víctimas y, posteriormente, les solicitan un rescate para devolvérselos, constituyendo una de las principales vías de extorsión utilizadas por los ciberdelincuentes a entidades empresariales, gubernamentales o personas físicas.

En la actualidad existe un tipo delictivo emergente denominado comúnmente "*Medusa*" cuyas víctimas principales son entidades gubernamentales, empresariales y económicas. Mediante la instalación de *softwares* maliciosos, los atacantes roban información confidencial de los usuarios para, después, pretender que los afectados paguen un precio para recuperarlos. En 2023 se creó el *Medusa Blog*, una página web dedicada a la publicación de la información sustraída y por la que no se ha abonado ningún rescate. Según un estudio realizado por la empresa Unit42[23] dedicada a la protección de los usuarios frente a las actuales amenazas cibernéticas, este novedoso *ransomware* afectó aproximadamente a 74 organizaciones a nivel global en el año 2023, y donde más ataques se han sufrido sus ataques ha sido Estados Unidos.

2.3. Impacto global y el futuro de estos delitos

El Foro Económico Mundial *(World Economic Forum)*[24], ha elaborado un Informe sobre las perspectivas para este año 2025 en relación con la seguridad global en materia de ciberdelincuencia[25].

En el informe de 2024, la organización destacó la creciente preocupación ante este emergente tipo delictivo y la complejidad de la situación. Esta se ve alimentada por una serie de factores como son las tensiones geopolíticas, la rápida incorporación de las innovaciones tecnológicas y la dependencia de las cadenas de suministro, creando un entorno caracterizado por la incertidumbre sobre el futuro y la vulnerabilidad de los sistemas que, debido a su incremento y proliferación, requieren de una regulación mucho más extensa.

---

[23] *Vid.:* Galiette, A., & Santos, D. "*Medusa Ransomware Turning Your Files into Stone"*. Unit 42, Palo Alto Networks, 2024 (disponible en https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/; última consulta en 28/03/2025).

[24] *Vid.:* Markovitz, G., y Feingold, S. "*¿Qué es Davos? 7 datos interesantes sobre la Reunión Anual del Foro Económico Mundial"*. Foro Económico Mundial., 5 de diciembre de 2024 (disponible en https://es.weforum.org/stories/2024/12/que-es-davos-7-cosas-que-hay-que-saber-sobre-la-reunion-anual-del-foro-economico-mundial/; última consulta en 26/03/2025).

[25] *Vid.:* World Economic Forum. "*Informe de Riesgos Globales 2025: Conflictos, medioambiente y desinformación, principales amenazas"*. Foro Económico Mundial, 2025 (disponible en https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/; última consulta en 25/03/2025).

En este contexto conviene introducir el concepto de ciberespacio que, tal y como se refiere a él la Directiva de Defensa Nacional de España del año 2020, se trata de *"el nuevo recurso crítico de la economía mundial" (Presidencia del Gobierno de España, 2020)*[26]. El Secretario General de Política de Defensa de España, el Almirante Juan Francisco Martínez Núñez, comentó en el XXXII seminario internacional de seguridad y defensa[27] este concepto en relación con la seguridad nacional y las futuras amenazas que podría suponer, determinando que el ciberespacio es *"donde se encuentran nuestros datos" (Martínez Núñez, 2020, p.26)*.

Por su parte, la Directiva del 2020, entra a cuestionar la soberanía del ciberespacio debido a ser este un ámbito común de todos los Estados sin fronteras físicas. En esta línea comenta que, esto dependerá de los medios que posea cada país en materia de conocimientos y regulación de accesibilidad a las TIC y, de sus ciudadanos, para poder garantizar un funcionamiento correcto y seguro a los consumidores mediante la cooperación intergubernamental de los Estados.

Dña. Paz Esteban, directora del Centro Nacional de Inteligencia (CNI), en este mismo seminario hace referencia a la verdadera sobreabundancia de información a la que nos enfrentamos[28]. Esta situación nos obliga a progresar al mismo tiempo sobre los medios informáticos que permitan el procesamiento de todos estos datos, así como sobre los sistemas que posibiliten su accesibilidad y distribución segura. Se advierte que, esta revolución digital, además de conllevar novedades favorecedoras y la incorporación de facilidades y utilidades para el día a día, también supone un nuevo medio para ataques a sus usuarios, los denominados *"enemigos sin rostro" (Esteban, 2020, p.38)*[29]. Con esto hace referencia a aquellos que hacen uso de los nuevos avances tecnológicos para, a través de ellos, captar y comprometer información tanto de personas físicas individuales como de entidades empresariales, administraciones o entes nacionales e internaciones.

---

[26] *Vid.:* Presidencia del Gobierno de España. (2020). *Directiva de Defensa Nacional 2020*. Gobierno de España.

[27] *Cfr.:* XXXII Seminario Internacional de seguridad y defensa - Amenazas desde el Ciberespacio, Madrid, Septiembre de 2020 (disponible en https://repositorio.comillas.edu/xmlui/handle/11531/55854, última consulta en 28/03/2025).

[28] "*Nos enfrentamos a una verdadera sobreabundancia de información que nos obliga a aumentar y modernizar nuestra capacidad para procesarla, tratarla, almacenarla, hacerla accesible, distribuirla y explotarla" (Esteban, 2020, p.36).*

[29] Esteban, P., XXXII Seminario Internacional de seguridad y defensa - Amenazas desde el Ciberespacio, Madrid, septiembre de 2020, p. 38 (disponible en https://repositorio.comillas.edu/xmlui/handle/11531/55854, última consulta en 28/03/2025).

Esta emergente tipología delictiva tiene la peculiaridad de que puede realizarse desde cualquier lugar del mundo con un alto nivel de anonimato por parte del atacante, el cual, detrás de los asaltos a los sistemas de información, suele tener como finalidad *"el espionaje, la desestabilización, el robo, la extorsión o la suplantación de la identidad de personas físicas o jurídicas" (Esteban, 2020, p.38)*[30].

Todo este rápido desarrollo del ciberespacio en el que nos encontramos ha generado diferencias entre organizaciones grandes y pequeñas en relación con su *"resiliencia cibernética"*, siendo esto la capacidad de las organizaciones para evolucionar en su desarrollo normativo, de prevención y recuperación ante amenazas y ataques cibernéticos[31].

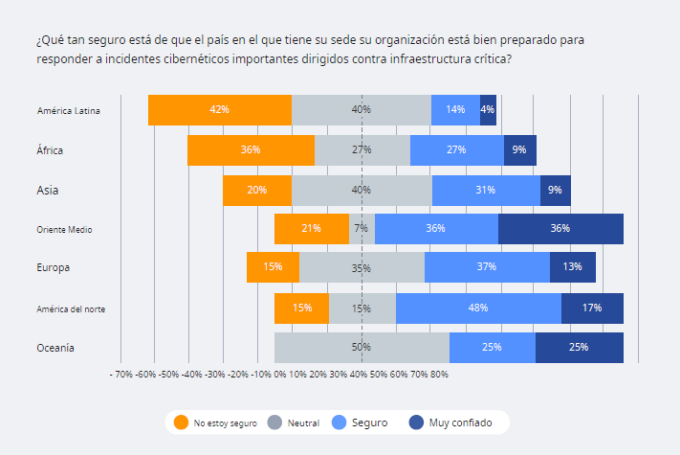
En la Reunión Anual sobre ciberseguridad de 2025 organizada por el Foro Económico Mundial, se subrayó la creciente preocupación por la capacidad de protección ante amenazas de las pequeñas organizaciones. En las encuestas realizadas a diferentes países, resalta la gran discordancia que hay entre aquellos que se encuentran en Europa y América del Norte, frente a los situados en América del Sur y África. Mientras solo el 15% de los pertenecientes al primer grupo están preocupados por su capacidad de hacer frente a estas amenazas, en el segundo grupo son el 36% los que creen que no poseen ni los medios ni la preparación suficiente para combatir esto.

Esta diferencia también se ha detectado entre las empresas del sector privado y las entidades públicas encuestadas, de las cuales el 38% consideran que no cuentan con una resiliencia suficiente, frente a sólo el 10% de las privadas que cuestiona dichas capacidades.

---

[30] *Id.*

[31] *Vid.:* World Economic Forum. "*5 maneras de lograr una resiliencia cibernética efectiva", noviembre de 2024 (disponible en* https://es.weforum.org/stories/2024/11/5-maneras-de-lograr-una-resiliencia-cibernetica-efectiva/; última consulta 28/03/2025).



(Foro Económico Mundial, 2025, p. 15)

En el informe se exponen las principales dificultades que se deberán de tratar en este año 2025 y que son las siguientes:

I. *"Vulnerabilidades de la cadena de suministro"*[32], que se conforma como la principal amenaza ante el desarrollo de la resiliencia cibernética debido a la ausencia de supervisión y su complejidad, desencadenando esto en posibles ciberataques o softwares con brechas que serán más fácil de atacar.

II. Tensiones geopolíticas, como uno de los principales factores de preocupación para los directivos de las compañías en relación con la vulnerabilidad de los datos informáticos de las entidades y sus posibles consecuencias en el ámbito de la competencia internacional.

III. Mientras que el desarrollo de la inteligencia artificial (IA) y su rápido progreso ha supuesto grandes avances en diferentes ámbitos, la mayoría de los países encuestados (un 63%) apuesta por sistemas de seguridad que permitan evaluar la fiabilidad de estas herramientas antes de incorporarlas a sus organizaciones, debido a que esta herramienta está suponiendo también una ayuda para la comisión de delitos cibernéticos más sofisticados. Asimismo, se ha incrementado

[32] La cadena de suministro, también denominada como *"supply chain"*, hace referencia a todas las actividades realizadas para que los productos o servicios lleguen al cliente de la mejor manera posible. Principalmente está compuesta por la obtención de la materia, su posterior transformación, los servicios de almacenaje, transporte y su final entrega al cliente o punto de venta. Estos procesos actualmente se encuentran controlados a través de programas informáticos que contienen información delicada de las empresas que se ven amenazados por los ciberdelincuentes, siendo uno de los principales focos los sistemas utilizados por los pequeños proveedores.
Vid.: Telefónica. "*Ciberseguridad en la cadena de suministro: mejor protección y políticas"*. Blog de Telefónica, s.f. (disponible en https://www.telefonica.com/es/sala-comunicacion/blog/ciberseguridad-cadena-de-suministro-mejor-proteccion-y-politicas/; última consulta en 28/03/2025).

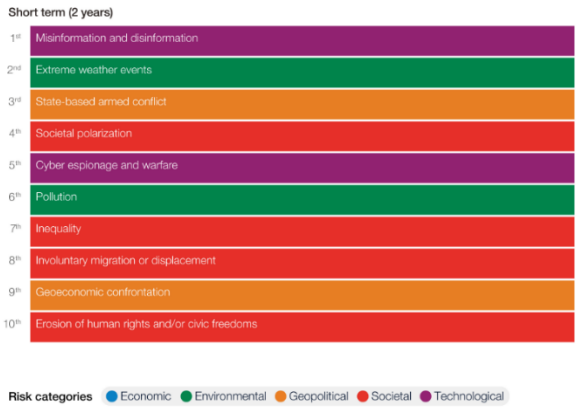
la demanda laboral de personas con habilidades y conocimiento en estos avances ya que debido a los continuos cambios que se producen, se busca la creación de nuevas estrategias para combatir estas amenazas.

IV. El *ransonware* continúa siendo la principal preocupación en el panorama mundial seguido del fraude cibernético. Como menciona Ivan John E. Uy, secretario de las TIC de Filipinas, "*A medida que se amplía nuestra huella digital, también lo hace la superficie de ataque potencial para actores maliciosos. Es esencial que trabajemos juntos para abordar esta creciente amenaza. La naturaleza sin fronteras de Internet requiere la colaboración entre distintas jurisdicciones para garantizar que los actores de amenazas no tengan un refugio seguro para sus actividades maliciosas" (Uy, 2025, p. 14)*[33].

V. El rápido crecimiento, junto con el cambio de las corrientes tecnológicas, es considerado como un obstáculo ante el progreso de la ciberresiliencia y la disminución de las diferencias entre los diferentes países, derivando en la sofisticación de la actividad delictiva y las tensiones geopolíticas. En este marco mundial ante el que nos encontramos el informe declara que, en orden a hacer frente a estas amenazas, en primer lugar, es indispensable que haya unanimidad entre los líderes empresariales sobre cuáles son los principales riesgos, priorizando la colaboración para el alcance de soluciones conjuntas calificándose la ciberseguridad como una responsabilidad común.

En el *"Informe de Riesgos Globales 2025: Conflictos, medioambiente y desinformación, principales amenazas"* realizado por el *Word Economic Fórum,* se presentan los principales riesgos a nivel mundial a corto y largo plazo ordenados según la gravedad de la situación. Este se basa en los resultados de más de 900 opiniones de expertos en relación con las amenazas mundiales, de los cuales, la mayoría prevén una situación global futura marcada por los cambios tecnológicos, medioambientales y sociales, para lo que será necesario reforzar la cooperación intergubernamental.

[33] Uy, I. J. E. "*Foro Económico Mundial*, *Perspectivas mundiales de ciberseguridad para 2025"* (p. 14), 2025 (disponible en https://es.weforum.org/publications/global-cybersecurity-outlook-2025/; última consulta en 28/03/2025).



(World Economic Forum, 2025)[34]

Como se refleja en el gráfico, las situaciones que involucran el desarrollo tecnológico se encuentran en el primer y quinto puesto de amenazas que más preocupan en un plazo de dos años. La desinformación y el ciberespionaje suponen un riesgo tanto para personas físicas como jurídicas y entidades gubernamentales, vulnerando los derechos individuales a la intimidad y la libertad, protegidos por nuestra Constitución Española en su artículo 18.4 en el que dispone que *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

Mark Elsner, responsable de la Iniciativa de Riesgos Globales del Foro Económico Mundial, refleja ante esta perspectiva su preocupación afirmando que *"nos enfrentamos a crisis interconectadas que exigen una acción coordinada y colectiva"*[35]*,* animando a fomentar la cooperación internacional para frenar estas amenazas que podrían tener consecuencias que perdurarían durante generaciones.

Las amenazas a los Sistemas de la Información y la Comunicación no son un caso aislado, sino que requieren de una cooperación internacional efectiva. Por otro lado, el impacto de la inteligencia artificial puede suponer un medio muy beneficioso para la creación de medidas de seguridad, siempre dependiendo del uso que le demos. Esta herramienta podríamos decir que es de "doble filo", ya que estos avances son comúnmente utilizados

[34] World Economic Forum. "*Global risks ranked by severity* [Infografía]. En *Global Risks Report 2025*", World Economic Forum, 2025 (disponible en https://es.weforum.org/publications/global-cybersecurity-outlook-2025/ ; última consulta en 28/03/2025).
[35] Elsner, M. "*Declaración sobre los riesgos globales y la cooperación internacional"*. Foro Económico Mundial, 2025

en la creación de sistemas y programas informáticos cada vez más sofisticados[36]. En este ámbito, los Estados deberían de fomentar el desarrollo e implementación de la IA mediante programas de enseñanza, con el objetivo de mejorar la resiliencia cibernética de los Estados anteponiéndose a las posibles amenazas, fomentando también la disminución de la brecha digital entre países desarrollados y aquellos en vías de desarrollo.

Esto, unido los continuos cuestionamientos sobre la soberanía en el ciberespacio, deriva en un ambiente de tensiones y diálogos políticos por su dominio, por lo que una rápida y eficaz normativa internacional debería de ser de carácter urgente.

3. El Convenio de Budapest sobre la Ciberdelincuencia: importancia, beneficios y sus protocolos adicionales

El Convenio de Budapest sobre la Ciberdelincuencia (en adelante, el Convenio), es considerado como el principal instrumento de cooperación internacional y armonización legislativa para la lucha frente a este emergente tipo delictivo.

El Convenio, impulsado por el Consejo de Europa en el año 2001, no limita su aplicación al ámbito europeo, sino que, además de aquellos que participaron en la negociación del texto (los miembros del Consejo de Europa junto con Canadá, Japón, Estados Unidos y Sudáfrica), gracias a su art. 37 se permite la adhesión de cualquier Estado[37].

Este se encuentra dividido en 4 capítulos, en los que no reduce su contenido sólo a la ciberdelincuencia, sino que también se aplica a otros tipos de delitos para los cuales su medio de comisión son los equipos informáticos, como los dedicados a la pornografía infantil o, por el contrario, sean estos el objetivo del delito, como los fraudes informáticos o el robo de información.

El Convenio tiene como objetivo establecer un marco jurídico común en materia de ciberdelincuencia mediante la armonización legislativa de los Estados parte con la normativa internacional, de cara a disminuir las diferencias regulatorias sobre aquellos delitos que sean similares.

---

[36] *Vid.:* BBVA. "*La IA en los dos lados de la ciberseguridad: aliada y amenaza en el mundo digital",* s.f. (disponible en https://www.bbva.com/es/innovacion/la-ia-en-los-dos-lados-de-la-ciberseguridad-aliada-y-amenaza-en-el-mundo-digital/; última consulta en 27/03/2025).

[37] *Cfr.:* Consejo de Europa. "*Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios"*. Estrasburgo, Francia, 2022 (disponible en https://rm.coe.int/cyber-buda-benefits-junio2022-es-final/1680a6f9f4; última consulta en 25/03/2024).

El texto incorpora diferentes medios para conseguir la cooperación efectiva como una red de comunicación las 24 horas del día todos los días del año y medios de intercambio de información y de asistencia judicial, fomentando la investigación y seguimiento conjunto de los delitos. Para ello, el artículo 24 establece medidas para la extradición entre países parte de aquellos que puedan ser considerados sospechosos de actividades delictivas. Toda la regulación ofrecida para el tratamiento de estas actividades deberá de salvaguardar, entre otros, los derechos fundamentales de libertad de expresión y privacidad.

El Comité de la Convención sobre Delitos Cibernéticos (en adelante, T-CY) será el encargado de supervisar el buen funcionamiento, desarrollo e implementación del Convenio, representando a los Estados ante este. Las partes, conforme al art. 44, tienen la posibilidad de presentar enmiendas en relación con el texto, las cuales serán recibidas por el comité que expresará su opinión sobre las mismas de cara a la adopción o no de estas por el Comité de ministros del Consejo de Europa.

El T-CY tiene un papel de mediación frente a las diferencias interpretativas o de aplicación que se presenten entre las partes en relación con el texto del convenio. En el año 2024, el Convenio estaba ratificado por 77 Estados y se propuso su firma a 16 más. Todos los Estados que lo han ratificado tienen un papel dentro del comité, ya sea en calidad de miembros (aquellos que conforman los Estados parte), o en calidad de observadores (los nuevos signatarios y los que están en proceso).

Con el objetivo de conseguir un texto más completo, y complementar lo dispuesto en el convenio se incorporan dos protocolos adicionales.

El primero es el relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Suscrito el 28 de enero de 2003 en la ciudad de Estrasburgo, su finalidad es la de complementar el convenio de Budapest con normativa relativa *"a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos" (Consejo de Europa, 2003, p.2)*[38].

Mediante la implementación de estas regulaciones de carácter procesal con el objetivo de incorporar mejoras sobre la cooperación internacional, las partes se verán compensadas

[38] Consejo de Europa. "*Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos* (STE 189)". Estrasburgo, 2003.

con una mayor seguridad jurídica a través de un marco jurídico más completo que proporciona directrices específicas para este tipo de delitos en el marco del ciberespacio. Por otro lado, al igual que se establece una tipificación específica para aquellos que cometan acciones de carácter racista y xenófobo, también proporciona una mayor protección a las víctimas de este tipo de delitos tanto a nivel nacional como transfronterizo, animando a una mayor cooperación internacional para su persecución.

Las medidas adoptadas por el protocolo buscan el equilibrio ente la libertad de expresión y las sanciones impuestas sobre los actos de carácter racista, considerados como una violación de los derechos humanos y una fuente de desestabilización del Estado de Derecho.

El artículo 6, entre una de las medidas contenidas en el protocolo, solicita que las partes adopten medidas para tipificar las conductas que consistan en *"difundir o poner a disposición del público de otro modo, por medio de un sistema informático, material que niegue, minimice burdamente, apruebe o justifique actos constitutivos de genocidio o crímenes contra la humanidad".* En relación con esto, las partes podrán imponer excepciones para su tipificación como, en primer lugar, exigir que estas acciones se realicen con ánimo discriminatorio o promoviendo el odio o la violencia creando así un perjuicio directo sobre el o los afectados o, por otro lado, podrán decidir no incorporar dicha regulación en sus ordenamientos reservándose el derecho.

El segundo protocolo *"relativo a la cooperación reforzada y la divulgación de pruebas electrónicas"*[39] *(Consejo de Europa, 2022),* en 2024 ya se encontraba firmado por 46 Estados y ratificado por 2. Este, ofrece reforzar la cooperación tanto entre los Estados parte como entre el sector privado. Mediante esto, se busca desarrollar mayor rapidez en el intercambio de información, como pruebas electrónicas que sean de ayuda para investigar los diferentes delitos, uniendo las fuerzas de las autoridades junto con la de los proveedores privados de internet con el objetivo de obtener datos relacionados con las actividades en línea.

El protocolo incorpora medidas para aquellos casos que se consideren de emergencia y necesiten una respuesta rápida por parte de las autoridades, establecido principalmente en

[39] Consejo de Europa. "*Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas* (STE 224)". Estrasburgo, 2022 (disponible en https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80291; última consulta en 29/03/2025).

los artículos 9 y 10 del texto. Se prevén procedimientos acelerados para estas situaciones en las que las autoridades podrán obtener con mayor rapidez datos almacenados mediante una solicitud, la cual será presentada por medio del sistema establecido en el art. 35 del Convenio de Budapest a través del cual se garantiza una comunicación efectiva las 24 horas durante los 7 días de la semana (24/7). Las solicitudes deberán de contener la información específica sobre qué datos de solicitan, a quién y para qué cuestión o finalidad. Los Estados podrán poder condiciones previas al otorgamiento de esta información, así como también tendrán capacidad de denegarlo en caso de tener un motivo los suficientemente justificado en orden a su ordenamiento interno.

La implementación de estas medidas para incrementar la rapidez en la transmisión de información y pruebas electrónicas fomenta la cooperación internacional, aumentando la eficacia de las actividades de lucha contra ciberdelitos que nos entienden de barreras físicas y que cada son vez más sofisticados. El desarrollo de normativa relacionada con la privacidad en línea y la protección de datos debe de ser acorde con los derechos humanos asegurándose de que las medidas tomadas para la lucha contra la ciberdelincuencia a su vez sean lo suficientemente proporcionales y justas para no socavar los derechos y libertades individuales.

4. La Organización de Policía Criminal (INTERPOL)

4.1. La organización

La INTERPOL es una organización intergubernamental cuyas siglas hacen referencia a la Organización Internacional de Policía Criminal. Esta entidad tiene como finalidad la cooperación con la policía ejerciente de los 196 países miembros para velar por la seguridad global.

El organismo está formado por la Secretaría General, al frente de la cual se encuentra un secretario general. Este órgano, con sede en la ciudad de Lyon, se encarga de coordinar toda la actividad policial diaria con los países miembro mediante la gestión y análisis de bases de datos, así como con el apoyo e investigación de casos contra la delincuencia.

En cada uno de los países miembros se encuentra una Oficina Central Nacional (OCN), las cuales sirven de nexo con la Secretaría General. La OCN se dedica a la gestión a nivel nacional de los delitos, así como a la cooperación con aquellos casos transfronterizos.

Por último, la INTERPOL cuenta con una Asamblea General, donde se reúnen una vez al año todos los países miembros mediante uno o más delegados para la aprobación de programas de actuación y medidas contra las principales amenazas para garantizar el correcto funcionamiento de la organización y seguir manteniendo la seguridad internacional. Las decisiones se toman a través del sistema de mayoría simple o mediante el de dos tercios en función del tema a tratar, representando cada país un voto.

En el año 2017, la Asamblea General de la INTERPOL en su reunión que tuvo lugar en la ciudad china de Beijing, aprobó la posición de la organización al frente de la seguridad mundial con el objetivo de dar a conocer las labores de la INTERPOL a los gobiernos nacionales con el objetivo de cooperar con las diferentes entidades de carácter público y privado que formen parte de la red de seguridad internacional.

4.2. Objetivos, regulación y programas de lucha contra la ciberdelincuencia

La INTERPOL constituye la organización internacional de policía criminal más grande del mundo y, estableció en el año 2018 una serie de objetivos conocidos como *"Objetivos Globales de Policía",* con el objetivo de fortalecer la cooperación internacional en materia de seguridad y justicia penal ante el incremento de la delincuencia transfronteriza y amenazas en un mundo cada vez más digitalizado.

El primer objetivo establecido por la organización es la lucha contra el terrorismo, mediante la cooperación para el intercambio de información relacionada con actividades terroristas de cara a lograr una mayor rapidez en las respuestas y neutralizaciones de las amenazas. Como segundo objetivo, la INTERPOL trabaja para desmantelar las actividades desarrolladas a través de redes organizadas transnacionales que tengan relación, entre otros aspectos, con el tráfico de drogas, armas y personas. El debilitamiento de estas estructuras se busca mediante operaciones en colaboración con otros países e instituciones.

En tercer lugar, la organización también busca el bienestar de las víctimas de estos delitos, estableciendo como tercer objetivo la protección de las comunidades vulnerables promoviendo la justicia y protección penal y social ante aquellos que hayan sufrido las consecuencias de estas redes.

Como cuarto y sexto objetivo, la INTERPOL promueve la mejora de las tecnologías para el desarrollo de nuevas capacidades policiales de investigación y análisis de datos para hacer frente a las emergentes amenazas cibernéticas en este mundo cada vez más

digitalizado ofreciendo también cursos formativos para los agentes que deban actuar en estos campos.

En quinta posición, la INTERPOL apoya la mejora por parte de los Estados Miembros de sus políticas transfronterizas de cara a gestionar la seguridad de las mismas mediante un sistema de intercambio de información eficaz que permita rápidas respuestas ante escenarios de inmigración y tráfico ilícito de personas y mercancías.

Todos estos objetivos no serían posibles sin el último de ellos, la cooperación entre países para la organización conjunta de operaciones policiales ante aquellos delitos transnacionales que afecten a varios estados a la vez.

Estos objetivos constituyen una estrategia completa para abordar los actuales retos relacionados con la seguridad internacional que están causando más preocupación. Mediante la colaboración, innovación tecnológica y unos objetivos comunes, se busca el fortalecimiento de las medidas de seguridad de cara a preservar la justicia y la seguridad global.

Estos objetivos fueron respaldados por la Asamblea de la INTERPOL en su resolución número 6 a raíz de la reunión celebrada en Beijing en 2017. En esta, el presidente de la organización hizo referencia a las *"cuatro piedras angulares de gran importancia estratégica" (Meng, 2017)*[40] para el progreso de la INTERPOL y la supervivencia de su posición frente a la seguridad mundial. En su discurso indicó, que *"la segunda piedra angular consiste en la lucha contra la ciberdelincuencia"*[41] considerando que todos los delitos internacionales graves que vendrían en los próximos años estarían indudablemente relacionados con el internet.

Posteriormente, en el año 2023, la Asamblea se pronunció en la reunión celebrada en Viena a través de su resolución número 12, reconociendo de nuevo la importancia de estos objetivos y reflejando la necesidad de proponer una revisión sobre los mismos, así como de valorar los mecanismos del momento en materia de "*intercambio de datos policiales*"[42]

---

[40] Meng, H. "*Ir con los tiempos y mantener las esperanzas de un siglo - Una INTERPOL que mira al futuro"*. Discurso en la 86ª reunión de la Asamblea General de INTERPOL, Beijing, China. INTERPOL, 2017 (disponible en https://www.interpol.int/es/content/download/5351/file/17Y1721%20S%20DISCURSO%20PRESIDENTE%2086%20REUNION%20AG.pdf; última consulta en 30/03/2025).

[41] *Id.*

[42] Organización Internacional de Policía Criminal [INTERPOL]. "*Resolución nº 12: Cien años - Avanzar juntos hacia una convergencia estratégica mundial para el establecimiento de una arquitectura integrada de seguridad (GA-2023-91-RES-12)"*. INTERPOL, 2023.

(Organización Internacional de Policía Criminal [INTERPOL], 2023) de cara a mejorar su funcionamiento y aplicación.

Ante el panorama mundial, la INTERPOL, en línea con el cuarto objetivo mencionado anteriormente, elabora un marco estratégico con una duración de 4 años, siendo el último publicado para los años del 2022 al 2025, en el que se incluye una valoración de la situación, así como los objetivos para los próximos años. En el último acuerdo se fijan 4 objetivos, así como los efectos que se prevén alcanzar con ellos:

I. Desarrollo del conocimiento en materia de ciberdelincuencia y la situación actual de las amenazas en orden a desarrollar planes de prevención ante los ataques. Con esto, se busca mejorar la calidad de la información mediante la implementación de fuentes más fiables, así como reforzar la cooperación entre los países para el intercambio de la misma.
II. Mejora de las medidas de prevención, detección y desactivación de las amenazas y ataques mejorando la resiliencia cibernética, con el objetivo de ofrecer una mayor protección a los estados mediante la cooperación policial a nivel mundial para la desactivación de grupos criminales organizados.
III. Reforzar la labor policial mediante la creación de alianzas con el resto de los países miembro fomentando el desarrollo de soluciones y estrategias de cooperación como la creación de asociaciones para el fomento de la confianza dentro del ambiente cibernético mundial actual. Con ello se prevé el incremento y mejora de los países para la lucha contra la ciberdelincuencia mediante el uso de los medios proporcionados por la organización y la colaboración entre los países a través de proyectos conjuntos.
IV. Mejorar el rendimiento y los mecanismos de la organización mediante la participación y colaboración activa en foros internacionales para el desarrollo de la posición de la INTERPOL ante el panorama mundial en este ámbito, así como reforzar su posición ante los países y las amenazas.

La INTERPOL trabaja en el desarrollo de políticas y servicios con el objetivo de apoyar a los Estados y en los acuerdos bilaterales o multilaterales alcanzados entre estos, contando con una posición decisiva en el ámbito de la lucha contra la ciberdelincuencia en orden a garantizar e implementar políticas de cooperación internacional.

La asistencia de la INTERPOL no se limita a servir simplemente como medio de interconexión entre países, sino que ofrece medidas y protocolos para el desarrollo de investigaciones, así como herramientas para facilitar el trabajo de sus miembros. Los sistemas de la interpol han sido de gran utilidad para la conclusión de numerosas operaciones relacionadas con la ciberdelincuencia gracias a, por ejemplo, su gran base de datos.

Otro de los mecanismos a destacar son los Equipos de Respuesta a Incidentes (IRTs). Con este sistema, la INTERPOL garantiza una asistencia rápida y eficaz por parte de un equipo especializado para este tipo de investigaciones en el Estado que lo haya solicitado.

Uno de los proyectos clave recientes de la INTERPOL ha sido la operación *Africa Cyber Surge II* en colaboración con AFRIPOL[43]. Esta es considerada como un mecanismo policial regional de la Unión Africana que juega un papel importante en la cooperación internacional para la lucha de la delincuencia transnacional. La operación consiguió desactivar redes maliciosas que se dedicaban al phishing y al robo de datos empresariales gracias a la eficiente colaboración entre las agencias internacionales, nacionales y el sector privado. La operación concluyó con 14 arrestos y el descubrimiento de la red de delincuencia que se encontraba tras las pérdidas de casi cuarenta millones de dólares de diferentes entidades.

La detección de nuevas actividades u operaciones delictivas se harán llegar a los Estados por medio de "Alertas" a través de la plataforma de comunicación 24/7 establecida. El artículo 8 del Reglamento de INTERPOL sobre el Tratamiento de Datos enuncia este procedimiento. La información compartida podrá ser de utilidad para investigaciones independientes en curso de los Estados y, además, toda la información se recogerá en las bases de datos de la INTERPOL disponibles para la comunidad internacional. El sistema de alertas y notificaciones[44] permite informar sobre nuevas amenazas, modus operandi y delincuentes reconocidos al resto de países.

Los Sistemas de datos de la INTERPOL se clasificarán por grados de confidencialidad en orden a los perjuicios a los que pueda conllevar su divulgación por lo que, en función de

---

[43] *Cfr.:* INTERPOL. "*Cybercrime: 14 arrests, thousands of illicit cyber networks disrupted in Africa operation"*. INTERPOL, 2024 (disponible en https://www.interpol.int/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation; última consulta en 22/03/2025).

[44] *Vid.:* Título 3, Capítulo II, Sección 3ª del *Reglamento de INTERPOL sobre el Tratamiento de Datos*. Organización Internacional de Policía Criminal (INTERPOL).

esto, habrá información que sólo estará disponible para un grupo determinado de personas, Estados u organizaciones. Conforme al artículo 112 del Reglamento de INTERPOL sobre el Tratamiento de Datos estos grados son: *"INTERPOL – EXCLUSIVAMENTE PARA USO OFICIAL; "INTERPOL – USO RESTRINGIDO; INTERPOL – CONFIDENCIAL";* o, en el caso de no estar clasificado en alguno de estos, se encontrarán en *"INTERPOL – EXCLUSIVAMENTE PARA USO OFICIAL".*

Esta clasificación podrá ser modificada por la Oficina Central Nacional en base a los análisis realizados sobre los riesgos que pueda conllevar la publicación de la información, siendo estas también las únicas que podrán dar acceso la información contenida en los sistemas de la INTERPOL a las entidades que lo requieran.

5. La Organización de las Naciones Unidas (ONU)

5.1. Constitución y funcionamiento de la ONU

El 24 de octubre de 1945 se hace oficial el nacimiento de la Organización de Naciones Unidas (ONU), tras la ratificación de la llamada "Carta de la ONU" por los 51 países que formaron parte entonces ya que, actualmente, la organización cuenta con 193 Estados Miembros (EM).

La Carta de Naciones Unidas[45], a cuyo cumplimiento se adhieren y vinculan los EM, es considerada como uno de los elementos fundacionales de la organización. Entró en vigor el 24 de octubre del año 1945, casi 4 meses después de que se firmase en San Francisco la Conferencia sobre Organización internacional. El documento fija los objetivos de la organización que se llevarán a cabo en colaboración con los Estados Miembros y las diversas "organizaciones afiliadas conocidas como programas, fondos y agencias especializadas"[46] (Organización de las Naciones Unidas [ONU], s.f.). En su preámbulo reflejan su interés en crear un orden internacional caracterizado por la justicia y la igualdad en el que se vele por los derechos fundamentales del hombre y de los Estados Miembros mediante la cooperación ente estos.

El artículo 1 de La Carta establece los cuatro objetivos principales de la comunidad internacional. En base a éstos, se velará por una cooperación internacional basada en la

[45] Naciones Unidas. (1945). *Carta de las Naciones Unidas*. https://www.un.org/es/about-us/un-charter
[46] Organización de las Naciones Unidas. (s.f.). *El sistema de las Naciones Unidas*. Naciones Unidas. https://www.un.org/es/about-us/un-system

igualdad y el respeto de los derechos de cada Estado, con el objetivo de conseguir la mayor eficacia posible de las medidas adoptadas. Su principal objetivo es preservar la paz mundial y abordar los problemas de carácter "*económico, social, cultural o humanitario"* que se presenten y, para conseguirlo, la Organización de Naciones Unidas se reconoce como un nexo entre las naciones para alcanzar la armonización legislativa influyendo de manera positiva en la cooperación internacional para hacer frente a los retos que se presentan en el siglo XXI.

La ONU cuenta con diversos órganos[47] que, dentro de sus competencias, ayudarán al cumplimiento de estos objetivos. El primero de ellos es la Asamblea General, el cual se constituye como *"el órgano representante, normativo y deliberativo de la ONU"*[48] *(Organización de las Naciones Unidas [ONU], s.f.).* Entre los asuntos que se someten a debate y votación en este órgano están aquellos relativos al mantenimiento de la paz y seguridad mundial, los que tengan carácter económico y las decisiones relativas a la admisión de nuevos Estados Miembros a la organización.

El Consejo de Seguridad se encarga exclusivamente de preservar la paz y la seguridad de las naciones mediante el análisis y la detección de amenazas que puedan corromper esto. El Consejo será el encargado de mediar en el caso de posibles discordancias entre Estados, así como de imponer las sanciones adecuadas en los casos que consideren necesarios para preservar la paz y la seguridad, así como será competente para autorizar el uso de la fuerza en aquellos casos en los que lo estime necesario y proporcional a la situación.

Los conflictos legales internacionales, así como las cuestiones en materia de interpretación normativa serán resueltos por la Corte Internacional de Justicia (CIJ) de la Haya, mediante la emisión de dictámenes y resoluciones sobre las cuestiones planteadas.

Todos estos órganos colaboran para alcanzar los propósitos de la ONU. Como establece la Carta de las Naciones Unidas[49], la Organización tiene como propósitos la colaboración internacional con el objetivo de crear soluciones y políticas comunes para la resolución de conflictos que alteren la paz y estabilidad internacional. Para lograr esto, la

---

[47] *Vid.:* Organización de las Naciones Unidas (ONU). *"Organigrama del Sistema de las Naciones Unidas* [PDF]". Naciones Unidas, s.f. (disponible en https://www.un.org/es/pdf/un_system_chart.pdf; última consulta en 30/03/2025).

[48] *Vid.:* Organización de las Naciones Unidas. (s.f.). *Órganos principales de las Naciones Unidas*. Naciones Unidas. https://www.un.org/es/about-us/main-bodies

[49] Organización de las Naciones Unidas. (1945). *Carta de las Naciones Unidas*, Artículo 1. Recuperado de https://www.un.org/es/about-us/un-charter

colaboración entre los Estados Miembros y la Organización de Naciones Unidas actuarán acorde con los principios de buena fe, igualdad soberana y protección de los Derechos Humanos, ofreciendo ayuda a aquellos que Estados que actúen conforme a lo dispuesto en la Carta pudiendo ser expulsado como Miembro cualquier Estado que haya actuado en contra de estos principios.

En relación con el papel de la Naciones Unidas ante la implementación de los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 la Asamblea General, a través de la resolución 72/279 del 31 de mayo de 2018, persigue la mejora de sus sistemas para ofrecer asistencia a los países que les permitan alcanzar estos objetivos. Como instrumento nacional en cada Estado Miembro, se incorpora el Marco de Cooperación de las Naciones Unidas para el Desarrollo Sostenible, como mecanismo para implementar y armonizar las medidas nacionales con el derecho internacional[50].

5.2. Regulación y programas de lucha contra la ciberdelincuencia

5.2.1. La Oficina de Lucha contra el Terrorismo (OLCT)

Las Naciones Unidas cuentan con una unidad especializada en la protección internacional contra el terrorismo. Dentro de esta, se localiza un programa dedicado a la ciberseguridad cuyo objetivo se basa en el desarrollo de medios y capacidades para con los Estados Miembro y entidades privadas para la prevención de ciber delitos.

Toda persona que tenga a su alcance dispositivos electrónicos puede realizar un mal uso de estos produciendo daños tanto a nivel personal como a terceros. Esta es una principal preocupación de este departamento, el uso de la red y las nuevas tecnologías por terroristas para la instigación, captación de personas, obtención de subvenciones y planificación de estrategias para llevar a cabo actividades terroristas. Ante esta amenaza, los Estados Miembro señalan la importancia del compromiso y cooperación internacional en orden a establecer medidas de seguridad frente a estos peligros.

La Asamblea General de Naciones Unidas aprobó el 26 de junio de 2018 el "Examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo". En esta se busca el fortalecimiento de las medidas de seguridad en relación con los actos de terrorismo que

[50] *Vid.:* Organización de las Naciones Unidas. "*UN Sustainable Development Cooperation Framework Guidance"*, 2019 (disponible en https://unsdg.un.org/sites/default/files/2019-10/ES_UN%20Sustainable%20Development%20Cooperation%20Framework%20Guidance.pdf; última consulta em 20/03/2025).

puedan ser realizados a través de las redes. Se propone la colaboración activa con las diferentes plataformas digitales y entidades proveedoras de servicios tecnológicos para detectar y evitar la propagación de información relacionada con actividades terroristas. Estas acciones se prevén garantizando su proporcionalidad y legalidad para su correcto funcionamiento, evitando restricciones abusivas velando por el respeto de la libertad de expresión y los derechos humanos de la sociedad.

Los Estados Miembros han expresado su preocupación en relación con el incremento del uso de las TIC a nivel global. Debido a esto, la OLCT ha desarrollado un programa con el cual, mediante la colaboración de los estados y las organizaciones privadas, se prevé el desarrollo de medidas para paliar el crecimiento de la amenaza.

El Consejo de Seguridad de Naciones Unidas emitió el 23 de diciembre del año 2015 las conclusiones y los principios a los que se había llegado con los Estados y las organizaciones, en relación con la protección y lucha contra las amenazas de los combatientes terroristas extranjeros[51].

Este informe tiene como principal objeto el incremento del uso de la tecnología por los terroristas para sus actividades delictivas siendo una de las principales amenazas globales en el ámbito tecnológico. La digitalización de los datos es una práctica cada vez más común debido a la rapidez y comodidad para los usuarios, pero también supone peligros para la intimidad tanto de personas físicas como jurídicas.

El documento alienta a los Estados a revisar tanto la normativa interna como los mecanismos que posean en relación con la asistencia judicial recíproca en orden de mejorar la cooperación entre jurisdicciones para el tratamiento de casos relacionados con ciberdelitos, ya que este tipo delictivo no entiende de barreras ni fronteras físicas. Se resalta la necesidad de que los Estados Miembros avancen en el estudio y medios disponibles en materia forense y las TIC dentro de aquellos organismos que tengan como labor el control de los delitos cibernéticos y de terrorismo.

La OLCT trabaja para creación de medidas efectivas que permitan a los Estados Miembros identificar, localizar y frenar en sus desplazamientos a estos terroristas, así

[51] *Cfr.:* Consejo de Seguridad de las Naciones Unidas. S/2015/939: Principios Rectores de Madrid sobre combatientes terroristas extranjeros. Naciones Unidas, 2015 (disponible en https://docs.un.org/es/S/2015/939; última consulta en 20/03/2025).

como para ofrecer protección a las mujeres y los niños que se encuentren vinculados a estos grupos.

5.2.2. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)

La Oficina de las Naciones Unidas contra la Droga y el Delito lleva velando por la seguridad internacional de 150 países desde el año 1997.

Entre los temas a los que se dedica esta oficina se encuentra la ciberdelincuencia. Debido a su carácter transnacional y su continuo crecimiento, este tipo de delitos exigen una mayor coordinación entre los Estado, y por ende de las organizaciones y entidades internacionales, para poder crear políticas efectivas. La oficina ofrece también su apoyo a los Estados en materia de revisión y reformulación de sus sistemas legislativos, así como formación y cooperación a las fuerzas y cuerpos de seguridad en su lucha contra la ciberdelincuena[52] *(Oficina de las Naciones Unidas contra la Droga y el Delito, s.f.)*.

En esta materia, la UNODC ha desarrollado el Programa Mundial sobre Delito Cibernético, que tiene como finalidad cuatro objetivos. En primer lugar, aumentar la visibilidad y concienciación de los riesgos que generan las TIC. Por otro lago, pretende fomentar la creación de legislaciones comunes entre los estados que permitan dar respuestas unánimes e idóneas ante las dificultades que se presenten. Para esto, como tercer objetivo, se anima al desarrollo de las competencias necesarias para *"prevenir, interrumpir, investigar, procesar y juzgar los delitos cibernéticos de acuerdo con los estándares de derechos humanos"*. Y, por último, para lograr todo esto se intentará conducir a un ambiente internacional basado en la cooperación conjunta entre los estados, las entidades privadas y la sociedad civil.

La UNODC, ofrece a las organizaciones gubernamentales medios de prevención y protección frente a las amenazas de la ciberdelincuencia por lo que se incluye: *"una asistencia técnica que va desde la prevención a la resolución del delito; la detección a la presentación de pruebas digitales ante los tribunales; la recopilación y el análisis de pruebas; el apoyo a la investigación, el enjuiciamiento y la condena; en delitos ciber*

[52] *Vid.:* Oficina de las Naciones Unidas contra la Droga y el Delito. (s.f.). "*Ciberdelito"*, UNODC, s.f. (disponible en https://www.unodc.org/unodc/en/cybercrime/index_new.html; última consulta en 20/03/2025).

dependientes y ciber habilitados, incluidos el abuso y la explotación sexual de menores en línea y el uso delictivo/ilícito de activos virtuales"[53].

5.2.3. Normativa

I. Convención de las Naciones Unidas contra la ciberdelincuencia

El 24 de diciembre del año 2024 la Asamblea General de las Naciones Unidas aprobó, la Convención de las Naciones Unidas contra la Ciberdelincuencia, en la Resolución 79/243 de la Asamblea General de Naciones Unidas, *relativa al fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves*[54]

Previamente, la Asamblea General en su resolución número 74/247, en orden a obtener un estudio lo más completo posible sobre el delito cibernético, reflejó la necesidad de crear un comité intergubernamental abierto (también llamado Comité *ad hoc*) que estuviese compuesto por diferentes expertos en la materia, contando con representantes de todos los Estados parte. Cumpliendo con los dispuesto en la resolución, en mayo de 2021 tuvo lugar el periodo de sesiones de tres días en los que los miembros de comité acordarían los objetivos y las líneas a seguir para la elaboración de la convención, a raíz del cual se aprobó la resolución 75/282 titulada "Refuerzo de la utilización de las tecnologías de la información y las comunicaciones con fines delictivos".

En esta, la Asamblea establece que el comité deberá de convocar consultas entre periodos de sesiones, teniendo en cuenta las aportaciones realizadas, respetando y haciendo uso de los mecanismos ya existentes para la lucha contra la ciberdelincuencia. Asimismo, se solicita que, en colaboración con la UNODC, se elabore una lista de representantes que podrían adherirse al comité de diferentes organizaciones no gubernamentales, instituciones académicas y procedentes del sector privado, con el objetivo de contar con una representación lo más amplia posible.

---

[53] Oficina de las Naciones Unidas contra la Droga y el Delito. (2024). "*Global Programme on Cybercrime Training Catalogue"*. UNODC, 2024 (disponible en https://www.unodc.org/unodc/en/cybercrime/home.html; última consulta en 20/03/2025).

[54] Naciones Unidas. (2024). Convención de las Naciones Unidas contra la Ciberdelincuencia: Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves (A/RES/79/243). Naciones Unidas.

Cumpliendo con lo establecido en la Resolución, se celebraron seis sesiones de negociación. Durante el periodo de tiempo comprendido entre el 29 de enero y el 9 de febrero, tuvo lugar la sesión de clausura en la ciudad de Nueva York, donde se aprobó el borrador de la Convención Internacional Integral sobre la Lucha contra la Utilización de las TIC con fines delictivos.

La Sra. Ghada Waly, directora ejecutiva de la UNODC, hace referencia a las negociaciones de esta convención como *"un acontecimiento histórico, ya que se trata del primer tratado multilateral contra el crimen en más de 20 años y la primera Convención de las Naciones Unidas contra la Ciberdelincuencia, en un momento en que las amenazas en el ciberespacio crecen rápidamente" (Oficina de las Naciones Unidas contra la Droga y el Delito, 2024)*[55].

Como establece el artículo primero de la Convención, esta se realiza con la finalidad de promover, fortalecer y apoyar la cooperación internacional, la negociación e implementación de medidas, y la asistencia jurisdiccional mutua para la lucha contra las amenazas presentes por la ciberdelincuencia.

Los Estados Parte que formen parte de otros convenios, convenciones o protocolos de Naciones Unidas, serán responsables de tipificar como delitos conforme a su derecho interno, los contenidos en estos, siempre que sean realizados por medio de las TIC. Por otro lado, el texto establece la necesidad de que, en orden a su aplicación, los Estados deberán de respetar los principios de no intervención, igualdad y de soberanía del resto de Estados, así como deberán de velar por el cumplimiento y protección de los Derechos Humanos.

Las actividades que se criminalizan por la Convención son: el acceso ilícito a sistemas informáticos, el apoderamiento sin autorización de información confidencial, los actos que tenga como finalidad la alteración de los datos, el uso indebido de dispositivos o sistemas de acceso digitales y los aquellos que hagan uso de las TIC para la obtención, distribución o venta de contenido de materia sexual de menores y, por último, aquellos dedicados a la ocultación, compra o transmisión de bienes delictivos.

[55] Oficina de las Naciones Unidas contra la Droga y el Delito. "*Estados Miembro de las Naciones Unidas aprueban borrador para una convención contra la ciberdelincuencia"*. UNODC, agosto 2024 (disponible en https://www.unodc.org/lpomex/es/noticias/agosto-2024/estados-miembro-de-las-naciones-unidas-aprueban-borrador-para-una-convencion-contra-la-ciberdelincuencia.html; última consulta en 10/03/2025)

El artículo 21 establece la necesidad de que casa Estado imponga sanciones *"efectivas, proporcionadas y disuasorias"* a la hora de enjuiciar la comisión de los delitos tipificados en esta. De cara a establecer las circunstancias agravantes o atenuantes, los Estado adoptarán lo establecido en su legislación nacional, respetando los derechos y principios básicos establecidos en la presente Convención.

Los Estados tendrán jurisdicción sobre aquellos delitos que se cometan dentro de su territorio y sobre aquellos que se cometan en embarcaciones navales o en aeronaves que se encuentren sometidos a su legislación. Además, un Estado tendrá competencia jurisdiccional sobre aquellos delitos que se cometan por o contra un nacional suyo o que resida habitualmente allí, directamente contra el Estado mismo, o en otro, pero para llevar a cabo un delito contra él. En el caso de que dos o más Estados se encuentren trabajando o con procedimientos judiciales activos sobre un mismo caso, se anima a que coordinen sus acciones para evitar conflictos en materia jurisdiccional. Por otro lado, para la tipificación y sanción de estos delitos, siempre que actúen conforme a la normativa internacional y persigan la misma finalidad, los Estados podrán seguir aplicando su normativa interna al respecto.

En orden a facilitar la cooperación entre los Estados para el desarrollo de investigaciones y procesos judiciales, el artículo 40 establece los principios y procedimientos por los que deberán velar las partes para llevar a cabo una asistencia jurídica efectiva, siempre en orden a la normativa interna de cada Estado. Para esto, el convenio anima a la formalización de acuerdos bilaterales o multilaterales, en orden a establecer las formalidades necesarias para facilitar la cooperación en el intercambio de información e investigaciones.

Aun sin haberse realizado solicitud, un Estado podrá compartir información con otro en el caso de considerarse que podría serle de utilidad para investigaciones o procedimientos activos, siempre respetando la confidencialidad de los datos y actuando conforme al ordenamiento interno. Siguiendo la línea para el fomento de la colaboración, se prevé la extradición de personas cuyo testimonio o ayuda puedan ser útiles en investigaciones. En estos casos, la persona deberá de prestar su consentimiento, así como los Estados deberán de establecer un acuerdo por medio del que, el país receptor, se comprometerá a velar por la seguridad del trasladado sin poder restringirle la libertad.

Todas estas solicitudes de cooperación mutua serán recibidas por la autoridad central competente que haya designado cada Estado, el cual se encargará de comprobar que estas cumplen con los requisitos establecidos.
Respecto a los gastos, los costos comunes de la asistencia judicial recíproca son responsabilidad del Estado solicitado, salvo que los Estados decidan lo contrario. En situaciones de gastos elevados o excepcionales, los Estados deben dialogar para decidir cómo se financiarán estos cargos.

Los Estados establecerán un sistema de comunicación a tiempo real que deberá de estar disponible y operativo las 24 horas del día, los 7 días de la semana. Este sistema denominado *"Red 24/7"*, busca ofrecer asistencia intergubernamental lo más rápido y eficazmente posible, ayudando así a investigaciones o procesos judiciales en materia de ciberdelincuencia.
Como establece el artículo 41, la asistencia comprenderá la recopilación, conservación y suministro de datos electrónicos, así como la prestación rápida de asesoramiento especializado en la materia, o la localización de personas en paradero desconocido que podrían ser sospechosos por la comisión de delitos. Cada Estado velará por tener personal cualificado al frente de esta red, así como también podrán, de manera voluntaria, reforzar aquellas redes de contacto ya existentes, como *"las redes de funcionamiento continuo sobre delitos relacionados con computadoras de la Organización Internacional de Policía Criminal para una cooperación interpolicial rápida y otros métodos de cooperación mediante el intercambio de información"*.

Un Estado podrá solicitar a otra información sobre la localización de la información almacenada y la necesidad de que esta se conserve. Esto podrá realizarse siempre y cuando se haga por medio de una solicitud motivada que, posteriormente, el Estado receptor valorará la solicitud conforme a su derecho interno y podrá a disposición del solicitante los medios necesarios siempre y cuando no sea rechazada la solicitud por falta de motivación o por posibles problemas con la confidencialidad de los datos o la posible obstrucción de la investigación. En esta línea, también podrán solicitarse la búsqueda de información que se encuentre almacenada en los sistemas informáticos de otro Estado.

En comparación con el Convenio de Budapest de 2001, la nueva Convención sobre Ciberdelincuencia contiene un texto más detallado, incorporando nuevas modalidades

delictivas y, por lo tanto, nuevas medidas de protección y cooperación internacional. Esto se debe a que, el Convenio de Budapest, debido al ámbito temporal en el que se realizó, recoge los tipos básicos de infracciones que se podían cometer a través de las TIC, pero, con el paso del tiempo, a la hora de la negociación de la nueva Convención de la ONU, el desarrollo y modernización de los sistemas también ha supuesto nuevos ciberdelitos que se recogen de manera detallada en este último texto.

La Convención de la ONU, aun encontrándose en un estado pendiente de revisión y ratificación por los Estados para su entrada en vigor, se espera que tenga un mayor alcance en la comunidad internacional debido a la modernización de los sistemas y las medidas que incorpora para la lucha contra la ciberdelincuencia.

En materia de delitos realizados a través de las TIC en materia de pornografía infantil, el Convenio de Budapest se limita a penalizar las conductas dedicadas a la obtención, transmisión, posesión o difusión de este tipo de materiales contra menores de edad[56]. En la misma línea, la Convención de Naciones Unidas incorpora la penalización de las actividades previas a la obtención del material pornográfico, todas aquellas que se lleven a cabo para obtener el material sexual de menores[57].

En comparación con la red 24/7 de comunicación internacional, la cooperación internacional establecida a la Convención de Naciones Unidas será de aplicación también al *"al embargo preventivo, la incautación, el decomiso y la devolución del producto de esos delitos"*[58]. Estas cuestiones no están específicamente detalladas en el Convenio de Budapest, el cual aplicará el uso de la Red 24/7 para la obtención de pruebas electrónicas cual cualquier tipo de delito independientemente de si se considera como ciberdelito o no, lo importante es que las pruebas sean de carácter electrónico.

En materia de competencia jurisdiccional[59], la Convención de Naciones Unidas incorpora la posibilidad de que los Estados tengan competencia para ejercer su jurisdicción cuando el delito haya sido cometido contra un nacional suyo, independientemente de dónde se encuentre (art. 22.2 a)), a diferencia del Convenio de Budapest que no incorpora nada en relación con esta posibilidad. Esto podría plantear cuestiones y conflictos en matera

[56] *Vid.:* artículo 9 del Convenio de Budapest.
[57] *Vid.:* artículo 15 de la Convención.
[58] *Vid.:* artículo 3, *"Ámbito de aplicación"*, de la Convención de Naciones Unidas.
[59] *Vid.:* artículo 22 de la Convención de Naciones Unidas y el artículo 22 del Convenio de Budapest.

jurisdiccional, no quedando claro quién sería competente o permitiendo a otros Estados en determinadas situaciones obstaculizar procedimientos internos de otros países.

Por último, y en orden a ofrecer la máxima protección a los Derechos Humanos, el Convenio de Budapest con su normativa la preservación y cumplimiento de lo dispuesto en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y las Libertades Fundamentales de 1950 y el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966, tal y como recoge expresamente en su preámbulo, recalcando el respeto a los derechos de libertad de expresión e intimidad. En esta línea, también hace referencia a la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (1999), haciendo remisiones expresas a estos textos que ofrecen seguridad jurídica a los Estados y especifican aquellos Derechos por los que habrá que velar en el momento de aplicación de su normativa.

Por otro lado, la novedosa Convención de las Naciones Unidas deja en manos de los Estados Parte estas salvaguardas[60] sin establecer medidas específicas de cooperación internacional es esta materia y, en algunos casos, considerándose que el Convenio puede suponer problemas para la protección de los Derechos Humanos y la armonización normativa internacional[61].

6. Actuaciones conjuntas entre las organizaciones

Desde la resolución de la Asamblea General número 51/1 y su posterior confirmación mediante el acuerdo de cooperación de 1997, la INTERPOL cuenta con el papel de "observador permanente" dentro de la ONU. La cooperación entre estas dos organizaciones ha sido fundamental desde entonces, habiendo sido recordada en posteriores resoluciones internacionales, para la investigación principalmente de casos relacionados con el terrorismo o la trata de personas.

Con el objetivo de prosperar en la cooperación entre las organizaciones, así como de hace uso mutuo de los medios que ambas poseen, la INTERPOL en 2004 abrió "La Oficina del Representante Especial de INTERPOL ante las Naciones Unidas" estableciendo su

[60] *Vid.:* artículo 6 del Convenio de Naciones Unidas contra la Ciberdelincuencia.

[61] *Vid.:* Human Rights Watch. "*Tratado de la ONU contra la ciberdelincuencia: una amenaza en ciernes"*. Human Rights Watch, 19 de ocutubre de 2023 (disponible en https://www.hrw.org/es/news/2023/10/19/tratado-de-la-onu-contra-la-ciberdelincuencia-una-amenaza-en-ciernes; última consulta en 14/03/2025).

sede en la ciudad de Nueva York, donde se encuentra también la sede de la ONU. Por otro lado, en el año 2018 realizó otro acercamiento en la ciudad de Viena abriendo "La Oficina del Observador Permanente" donde la ONU posee también oficinas.

Como se ha mencionado anteriormente, la INTERPOL y la ONU tienen una estrecha relación en materia de cooperación principalmente en materia de terrorismo y trata de personas. La INTERPOL colabora con las diferentes oficinas de Naciones Unidas dedicadas a la investigación y desarrollo de actividades antiterroristas. En este ámbito es de gran relevancia el Pacto Mundial de Coordinación de la Lucha Antiterrorista del cual es miembro desde finales del año 2018. Este pacto es considerado como uno de los cimientos de Naciones Unidas que permite el desarrollo de uno de sus principales objetivos, velar por la paz y la seguridad Internacional y un gran paso hacia el afianzamiento de medidas contra esta actividad delictiva.

En relación con los delitos cibernéticos, la INTERPOL juega un papel importante en el desarrollo de la *"Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos*[62]*"(INTERPOL, s.f.).*

La Oficina de Lucha contra el Terrorismo (OLCT) de Naciones Unidas es la encarga del desarrollo de mecanismos dirigidos a las conductas ciber delictivas de agentes terroristas.

En vistas de colaborar con el mantenimiento de la paz y la seguridad de las Naciones Unidas, se han creado mecanismos de cooperación policial entre ambas organizaciones para reforzar los cuerpos de policías internacionales y ofrecer apoyo a los agentes de los Estados Miembros para la defensa del Estado de derecho y peligros transnacionales. En este ámbito, se ha colaborado en relación con el intercambio de información a través de medios tecnológicos con fines terroristas, constituyéndose como delitos de carácter transnacional que no cuentan con barreras físicas y pueden ser realizados desde cualquier lugar.

Dentro de los objetivos incluidos en la Agenda 2030 en búsqueda del desarrollo sostenible mundial (en adelante ODS), se han incluido varios de carácter policial en los que la INTERPOL posee una posición dominante e importante de colaboración. En concreto, el

[62] INTERPOL. "*Prioridades actuales en la colaboración entre las Naciones Unidas e INTERPOL"*. INTERPOL.(disponible en https://www.interpol.int/es/Nuestros-interlocutores/Socios-de-organizaciones-internacionales/INTERPOL-y-las-Naciones-Unidas/Prioridades-actuales-en-la-colaboracion-entre-las-Naciones-Unidas-e-INTERPOL; última consulta en 5/03/2025).

objetivo número 16 tiene como objetivo *"promover sociedades pacíficas e inclusivas, facilitar el acceso a la justicia para toda la población y crear instituciones eficaces, responsables e inclusivas a todos los niveles" (Naciones Unidas, s.f.)*[63].

El Consejo de Seguridad de Naciones Unidas, en su resolución número 2341 del año 2017[64] en relación con las crecientes amenazas a las infraestructuras nacionales e internacionales por parte del terrorismo, reconoce la eficacia de la asistencia por parte de la INTERPOL para la protección de estas. La resolución anima a la colaboración internacional para el intercambio de información en relación con movimientos y actividades terroristas para la preparación de políticas de prevención y respuesta. La dependencia recíproca de las infraestructuras supone una mayor amenaza ya que los daños tendrán un mayor impacto. Ante este panorama, el secretario general de INTERPOL Jürgen Stock declaró que *"Un ataque dirigido contra un punto vulnerable puede interrumpir o destruir numerosos sistemas vitales del país directamente afectado, ocasionando un efecto en cadena en todo el mundo"*[65].

La reciente resolución de la Asamblea General de Naciones Unidas del 12 de diciembre de 2024 (A/RES/79/136)[66] pone de manifiesto la situación actual de la cooperación entre la ONU y la INTERPOL. Estas dos organizaciones cuentan con un papel importante en orden a la asistencia que ofrecen a los Estados Miembros en situaciones de peligro y amenazas. La INTERPOL destaca por los servicios de prevención y formación que ofrece a aquellos que la soliciten, velando por los Derechos Fundamentales, la normativa internacional y nacional, contando con oficinas centrales en cada uno de los países son el objetivo de crear una red mundial de asistencia y comunicación 24/7.

Reflejando la preocupación por el incremento de la ciberdelincuencia y las medidas de apoyo para su prevención a las autoridades nacionales, pero teniendo en consideración los avances en sistemas de intercambio de información, alertas y bases de datos, se solicita

---

[63] Naciones Unidas. "*Paz, justicia e instituciones sólidas: Objetivo 16"*. Naciones Unidas, s.f., (disponible en https://www.un.org/sustainabledevelopment/es/peace-justice/; última consulta en 5/03/2025).
[64] Naciones Unidas. Resolución 2341 (2017) [Resolución del Consejo de Seguridad], 2017 (disponible en https://www.un.org/es/sc/documents/resolutions/2017.shtml; última consulta en 19/03/2025).
[65] INTERPOL. "*Una resolución de la ONU destaca el papel de INTERPOL en la protección de infraestructuras esenciales frente a los terroristas"*, 13 de febrero de 2017 (disponible en https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2017/Una-resolucion-de-la-ONU-destaca-el-papel-de-INTERPOL-en-la-proteccion-de-infraestructuras-esenciales-frente-a-los-terroristas; última consulta en 19/03/2025).
[66] Naciones Unidas. Resolución 79/136. Cooperación entre las Naciones Unidas y la Organización Internacional de Policía Criminal (INTERPOL) [Resolución de la Asamblea General], 2024 (disponible en https://undocs.org/es/A/RES/79/136; última consulta en 19/03/2025).

el refuerzo de la cooperación entre la INTERPOL y Naciones Unidas de cara a mejorar las respuestas ante situaciones de terrorismo, delincuencia organizada transnacional o igualdad de género.

Asimismo, se llama al incremento de la cooperación entre ambas a través de los sistemas establecidos de intercambio de información (red 24/7), de notificaciones y alertas, la actualización contaste de las bases de datos y análisis de las investigaciones criminales, recalcando la importancia de las políticas de acceso.

6.1. Obstáculos internacionales ante la cooperación para frenar el incremento de la ciberdelincuencia

Como se ha expuesto hasta ahora, la evolución de la tecnología ha creado un espacio digital que no entiende de fronteras físicas. Este nos ofrece infinidad de medios y utilidades para nuestro día a día, pero también supone una amenaza para la seguridad y la paz global, lo cual supone una de las principales preocupaciones actuales en las organizaciones internacionales.

En orden a conseguir una normativa sobre el uso de internet lo más igualitaria y respetuosa posible con los usuarios entre los Estados, entra en juego la cuestión de la "gobernanza de internet".

La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) define este concepto como *"el desarrollo y la aplicación complementarios de los gobiernos, el sector privado, la sociedad civil y la comunidad técnica, en sus respectivas funciones, de los principios, normas, reglas, procedimientos de toma de decisiones y actividades compartidos que dan forma a la evolución y uso de Internet"*[67].

Esta cuestión es muy controvertida debido al carácter descentralizado de internet, por lo que para su regulación es necesaria la colaboración activa de los estados y las organizaciones internacionales. Ante esta circunstancia tuvo lugar la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI). Esta reunión se celebró en dos fases diferentes, la primera tuvo lugar en Ginebra en el año 2003 y la segunda en Túnez dos años más tarde. En estas, los Estados expresaron su preocupación ante la creciente digitalización y, de cara a conseguir políticas comunes para alcanzar los

[67] *Vid.:* UNESCO. "*Internet Governance"*. UNESCO, s.f. (disponible en https://www.unesco.org/es/internet-governance; última consulta en 15/03/2025).

objetivos de desarrollo mundiales, reconocieron su *"deseo y compromisos comunes de construir una sociedad de la información centrada en las personas, inclusiva y orientada al desarrollo" (Internet Governance Forum, s.f.).*

Por todo esto, en la segunda fase de la CMSI en Túnez se estableció, en el artículo 72 de la Agenda de Túnez, la creación del Foro de Gobernanza de Internet de las Naciones Unidas (FGI), el cual no tiene competencia decisoria, pero fomenta el diálogo y la negociación ante los problemas planteados de cara a concertar políticas comunes de gobernanza entre los Estados con la finalidad *"de fomentar la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet"*[68].

Este 2025 se celebrará la reunión anual número 20 del FGI en el que, bajo el nombre "*Construyendo Gobernanza Digital Juntos*", se tratarán cuatro temas diferentes propuestos por los diferentes miembros.

La primera cuestión para tratar será aquella relativa a la "*Ciberseguridad y confianza, Gobernanza de datos, Inteligencia artificial, Medios y contenido, Derechos y libertades [Fortalecimiento de capacidades]",* con el objetivo de conseguir sistemas de comunicación y redes fiables y seguro buscando la resiliencia digital[69]. De cara a promover el crecimiento económico y la innovación tecnológica responsable, se tratará la "*Sostenibilidad ambiental y cambio climático, Asuntos económicos y desarrollo, Tecnologías emergentes e innovación, Inteligencia artificial, Temas técnicos y operativos".*

En tercer lugar y en relación con los Derechos Humanos, será objeto de diálogo los Derechos digitales de cara a conseguir *"un futuro digital inclusivo, abierto, sostenible, justo, seguro y protegido".* Y, por último, se tratará de continuar fomentando la cooperación entre los Estados interesados regulado las novedades en el ámbito digital y sus posibles amenazas, animando a una participación equitativa y dialogada de los gobiernos para conseguir políticas comunes.

---

[68] Internet Governance Forum. "*WSIS+20 and IGF+20 Review by the UN General Assembly 2025"*. Internet Governance Forum, 2025 (disponible en https://www.intgovforum.org/en/content/wsis20-and-igf20-review-by-the-un-general-assembly-2025; última consulta en 24/03/2025).

[69] *"La resiliencia cibernética va más allá de la ciberseguridad, la prevención de ataques o simplemente volver a las operaciones habituales: se trata de la capacidad de una organización para minimizar el impacto de incidentes cibernéticos significativos en sus metas y objetivos principales".* Foro Económico Mundial. "*Unpacking Cyber Resilience"*. Foro Económico Mundial, 2024 (disponible en https://es.weforum.org/publications/unpacking-cyber-resilience/; última consulta en 20/03/2025).

El secretario general de las Naciones Unidas, Antonio Guterres, publicó en el mes de junio de 2020 la *"Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital (A/74/821)"*[70]. Este informe sobre la situación actual en un mundo cada vez más digitalizado anima a tres cuestiones fundamentales: *"conectar, respetar y proteger"*.

Estos tres principios tienes como finalidad la preservación de los Derechos humanos en el ámbito digital ya que *"los derechos humanos existen tanto en línea como fuera de línea y deben respetarse cabalmente" (A. Guterres, 2020).* La resolución propone medios por los que garantizar el correcto uso de la red de cara a evitar intromisiones ilegítimas en la privacidad de los usuarios, promover un uso basado en el respeto de los derechos individuales.

Previamente a la realización de este informe de ruta por el Secretario General, en julio de 2018 se adoptó una resolución acerca de la *"Promoción, protección y disfrute de los derechos humanos en Internet"*.

El documento A/HRC/38/L.10 de la Asamblea General de Naciones Unidas reconoce la necesidad de promover la seguridad en los espacios digitales en orden de preservar la libertad de expresión y la privacidad en línea como unos de los principales derechos que se ven vulnerados en este entorno. Estos dos principios se encuentran relacionados entre sí, ya que la confidencialidad en el entorno digital es un factor necesario para poder reflejar la diversidad de opiniones.

En primer lugar, y ligado a esto, la organización internacional lucha contra la desinformación, como uno de los principales riesgos a nivel mundial, sin una pluralidad de medios de información no se estaría fomentando la creación de ideas y opiniones libres y fundamentadas. Con el objetivo de frenar esto, se condenan *"las medidas que, en violación del derecho internacional de los derechos humanos, impiden o perturban la capacidad de una persona para buscar, recibir o transmitir información en línea"* así como todas aquellas medidas adoptadas por los Estados Miembros que busquen restringir esta libertad fundamental pero reflejando su preocupación por la implementación de restricciones que alienten al incremento de la brecha digital entre géneros, limitando el

[70] Naciones Unidas. Informe del Secretario General sobre la cooperación internacional en la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos (A/74/821). 2020 (disponible en https://docs.un.org/es/A/74/821; última consulta en 23/03/2025).

acceso a los medios tecnológicos a las mujeres, menoscabando así los derechos de las mujeres.

Siendo reconocido internet como una herramienta de gran utilidad para muchas situaciones de la vida cotidiana, se promueve que los Estados Miembros pongan a disposición los medios necesarios para permitir el acceso a este de toda la población y, en especial, a aquellos que sufran de alguna discapacidad o en situaciones para fomentar el aprendizaje y fomentar la educación por medios digitales.

Según el informe *"Human Rights Council holds panel discussion on online violence against women human rights defenders"*[71] elaborado en 2018, *"las mujeres y las niñas tenían 27 veces más probabilidades de ser acosadas en línea que los hombres"*[72]. Este documento expresa las preocupaciones generales en cuanto al desarrollo tecnológico y las amenazas que puede ocasionar a los derechos fundamentales de los individuos, siendo complementado posteriormente por la hoja de ruta, la cual detalla cómo llevar a la práctica lo expresado por el Consejo de Derechos Humanos, persiguiendo la seguridad de las redes y su uso como un medio para el desarrollo de la sociedad e intentando evitar su conversión en una herramienta que promueva la desigualdad.

7. Conclusiones

Los delitos que utilizan las nuevas tecnologías y sus avances están en completo auge, constituyendo una de las principales amenazas actuales a nivel mundial. Debido a la cantidad de información y confianza que depositamos en los nuevos sistemas, los delincuentes utilizan cada vez estrategias más sofisticadas para engañar, extorsionar, obtener, transmitir, modificar y suprimir esta información, afectando tanto a particulares como a entidades empresariales, gubernamentales e internacionales. La ciberdelincuencia engloba una infinidad de actividades realizadas a través de diferentes sistemas informáticos, formas de actuación de los delincuentes y con diferentes finalidades. Esta modalidad delictiva no es un término universal, cerrado ni único, sino que, debido a la cantidad de actuaciones que recoge (como se ha descrito en el apartado 2 de este trabajo)

[71] *Vid.:* Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Human Rights Council holds panel discussion on online violence against women human rights defenders", 21 de junio de 2018.
[72] Secretaría General de las Naciones Unidas. "*Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital"* (Informe A/74/821). Naciones Unidas, 2020, P.14 (disponible en https://undocs.org/A/74/821; última consulta en 20/03/2025).

no tiene una definición oficial. Lo que sí queda aprobado y acreditado, tanto por los expertos como por las entidades gubernamentales, nacionales e internacionales, es que se trata de un delito de carácter transfronterizo que no entiende de barreras físicas, pudiendo cometerse desde cualquier lugar del mundo contra personas, entidades o infraestructuras de otro país diferentes.

El Convenio de Budapest supuso un hito en la legislación internacional debido a ser el primero que recogía regulación sobre esta novedosa actividad delictiva. Debido a su adopción en el año 2001 y los rápidos avances de las TIC, esta normativa y sus protocolos adicionales se pueden llegar a considerar limitados por lo que, a finales de 2024 se aprobó el borrador de la Convención de Naciones Unidas contra la Ciberdelincuencia. Si es cierto que este nuevo texto legal recoge nuevos ciberdelitos ampliando su alcance y medidas de cooperación internacional para hacer frente a las amenazas, se cuestiona su colaboración con la preservación de los Derechos Humanos y cuál será su acogida por la comunidad internacional.

Ante esta situación, la INTERPOL y las Naciones Unidas, por sus funciones, cuentan con un papel importante de cara a promover la paz y seguridad internacional mediante programas, sistemas y medidas de apoyo de alerta e investigación para con los Estados. La creación de la Oficina de Lucha Contra el Terrorismo (OLTC), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) de la ONU y los equipos de investigación de la INTERPOL, realizan una gran labor a la hora de prestar asistencia a los países ante las amenazas del ciberespacio e infinidad de delitos relacionados con el tráfico de drogas, personas, pornografía infantil o actividades terroristas entre otros.

Debido a la descentralización por la usencia de barreras físicas de estos delitos y la sofisticación de los medios utilizados para llevarlo a cabo, nos pone ante una situación mundial en la que es necesaria una armonización legislativa. Lo que debería de incorporar expresamente serían medidas en materia jurisdiccional, así como una normativa que vele por la protección de los Derechos Humanos en cualquier lugar del mundo de forma igualitaria, ya que los delitos en línea pueden llegar a atentar contra la libertad de expresión, la igualdad, la intimidad y la privacidad de la sociedad.

Para avanzar en este aspecto y conseguir una red de protección internacional fiable, competente y exitosa, podrían estudiarse medios que permitan la interconexión global

reduciendo las diferencias con países menos desarrollados. Con el objetivo de conocer más el ciberespacio y contar con profesionales competentes en la materia, se podrían implementar programas de financiación cuyo objetivo sea la creación de programas de investigación, estudio y formación acerca de las novedades informáticas y corrientes delictivas. Estos proyectos podrían tener como uno de sus principales objetivos la reducción de la brecha digital que, junto con la posible creación de un nuevo órgano internacional especializado, tendría como misión la "actualización" de los países en vías de desarrollo con material técnico y formación especializada.

La identificación de los sectores más vulnerables o que constituyen unos de los principales objetivos de los ciberdelincuentes, podría servir de ayuda para la creación de normativa especializada como, por ejemplo, regulación destinada a las entidades bancarias internacionales y las nuevas formas de inversión en línea.

8. Bibliografía

8.1. Legislación

Consejo de Europa. *"Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE 189)".* Estrasburgo, 2003.

Consejo de Europa. "Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (STE 224)". Estrasburgo, 2022 (disponible en https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80291; última consulta en 29/03/2025).

Consejo de Seguridad de las Naciones Unidas. S/2015/939: Principios Rectores de Madrid sobre combatientes terroristas extranjeros. Naciones Unidas, 2015 (disponible en https://docs.un.org/es/S/2015/939; última consulta en 20/03/2025).

Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia. (28 de mayo de 2014).

Naciones Unidas. (1945). Carta de las Naciones Unidas (disponible en https://www.un.org/es/about-us/un-charter; última consulta en 30/03/2025).

Naciones Unidas. Convención de las Naciones Unidas contra la Ciberdelincuencia: Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves (A/RES/79/243). Naciones Unidas, 2024 (disponible en https://digitallibrary.un.org/record/4071955/files/A_RES_79_243-ES.pdf; última consulta en 30/03/2025).

Naciones Unidas. Resolución 2341 (2017) [Resolución del Consejo de Seguridad], 2017 (disponible en https://www.un.org/es/sc/documents/resolutions/2017.shtml; última consulta en 19/03/2025).

Naciones Unidas. Resolución 79/136. Cooperación entre las Naciones Unidas y la Organización Internacional de Policía Criminal (INTERPOL) [Resolución de la Asamblea General], 2024 (disponible en https://undocs.org/es/A/RES/79/136; última consulta en 19/03/2025).

Naciones Unidas. Informe del Secretario General sobre la cooperación internacional en la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos (A/74/821). 2020 (disponible en https://docs.un.org/es/A/74/821; última consulta en 23/03/2025).

Organización Internacional de Policía Criminal [INTERPOL]. "Resolución nº 12: Cien años - Avanzar juntos hacia una convergencia estratégica mundial para el establecimiento de una arquitectura integrada de seguridad (GA-2023-91-RES-12)". INTERPOL, 2023 (disponible en https://www.interpol.int/es/content/download/20583/file/GA-2023-91-RES-12%20S%20Cien%20anos.pdf; última consulta en 30/03/2025).

Organización de las Naciones Unidas (ONU). (2024). "*Informe del Secretario General sobre la labor de la Organización"*, A/79/460 (disponible en https://docs.un.org/es/A/79/460; última consulta en 20/03/2025).

Presidencia del Gobierno de España. (2020). Directiva de Defensa Nacional 2020. Gobierno de España (disponible en https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf; última consulta en 15/03/2025).

Interpol. "*Rules on the Processing of Data (RPD) 2024"* (disponible en https://www.interpol.int/es/content/download/5694/file/27%20S%20RulesProcessingData_RPD_2024.pdf; última consulta en 30/03/2025).

8.2. Recursos de internet

BBVA. "La IA en los dos lados de la ciberseguridad: aliada y amenaza en el mundo digital", s.f. (disponible en https://www.bbva.com/es/innovacion/la-ia-en-los-dos-lados-de-la-ciberseguridad-aliada-y-amenaza-en-el-mundo-digital/; última consulta en 27/03/2025).

Centro de Formación de la Cooperación Española. *"La ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional (segunda edición)",* 2021 (disponible en https://goo.su/U2Ic1M4; última consulta en 30/03/2025).

Código de Vera. "*Ataque de intermediario (MITM)".* Código de Vera, s. f. (disponible en https://www.veracode.com/security/man-middle-attack/; última consulta 20/03/2025).

Consejo de Europa. *"Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios".* Estrasburgo, Francia, 2022 (disponible en https://rm.coe.int/cyber-buda-benefits-junio2022-es-final/1680a6f9f4; última consulta en 25/03/2024).

Consejo de los Ministerios de Justicia de los Países Iberoamericanos (COMJIB). *"Entra en vigor el Convenio Iberoamericano de Cooperación en materia de Ciberdelincuencia",* 17 de julio de 2023 (disponible en https://comjib.org/entra-en-vigor-el-convenio-iberoamericano-de-cooperacion-en-materia-de-ciberdelincuencia/; última consulta en 27/03/2025).

Galiette, A., & Santos, D. *"Medusa Ransomware Turning Your Files into Stone".* Unit 42, Palo Alto Networks, 2024 (disponible en https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/; última consulta en 28/03/2025).

Human Rights Watch. *"Tratado de la ONU contra la ciberdelincuencia: una amenaza en ciernes".* Human Rights Watch, 19 de octubre de 2023 (disponible en https://www.hrw.org/es/news/2023/10/19/tratado-de-la-onu-contra-la-ciberdelincuencia-una-amenaza-en-ciernes; última consulta en 14/03/2025).

IBM. *"Ransomware"*. IBM, s.f. (disponible en https://www.ibm.com/es-es/topics/ransomware; última consulta en 27/03/2025).

IBM. *"Suplantación de identidad (phishing). Phishing"*. IBM, s.f. (disponible en https://www.ibm.com/es-es/topics/phishing; 27/03/2025).

Real Academia Española. Política de cookies. Real Academia Española (s.f.) (disponible en https://www.rae.es/politica-de-cookies; última consulta 25/02/2025).

INTERPOL. *"Cybercrime: 14 arrests, thousands of illicit cyber networks disrupted in Africa operation"*. INTERPOL, 2024 (disponible en https://www.interpol.int/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation; última consulta en 22/03/2025).

INTERPOL. *"Prioridades actuales en la colaboración entre las Naciones Unidas e INTERPOL"*. INTERPOL. (disponible en https://www.interpol.int/es/Nuestros-interlocutores/Socios-de-organizaciones-internacionales/INTERPOL-y-las-Naciones-Unidas/Prioridades-actuales-en-la-colaboracion-entre-las-Naciones-Unidas-e-INTERPOL; última consulta en 5/03/2025).

INTERPOL. *"Urge actuar de inmediato para evitar una pandemia de ransomware"*, INTERPOL., 2021 (disponible en https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/Urge-actuar-de-inmediato-para-evitar-una-pandemia-de-ransomware-INTERPOL; última consulta en 27/03/2025).

INTERPOL. *"YoINTERPOL y UNICEF firman un acuerdo de cooperación para combatir la explotación y el abuso sexual de menores"*, 2023. (disponible en https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2023/INTERPOL-y-UNICEF-firman-un-acuerdo-de-cooperacion-para-combatir-la-explotacion-y-el-abuso-sexual-de-menores; última consulta en 27/03/2025).

INTERPOL. *"Una resolución de la ONU destaca el papel de INTERPOL en la protección de infraestructuras esenciales frente a los terroristas"*, 13 de febrero de 2017 (disponible en https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2017/Una-resolucion-de-la-ONU-destaca-el-papel-de-INTERPOL-en-la-proteccion-de-infraestructuras-esenciales-frente-a-los-terroristas; última consulta en 19/03/2025).

Internet Governance Forum. *"WSIS+20 and IGF+20 Review by the UN General Assembly 2025"*. Internet Governance Forum, 2025 (disponible en

https://www.intgovforum.org/en/content/wsis20-and-igf20-review-by-the-un-general-assembly-2025; última consulta en 24/03/2025).

Telefónica. *"Ciberseguridad en la cadena de suministro: mejor protección y políticas"*. Blog de Telefónica, s.f. (disponible en https://www.telefonica.com/es/sala-comunicacion/blog/ciberseguridad-cadena-de-suministro-mejor-proteccion-y-politicas/; última consulta en 28/03/2025).

Meng, H. "*Ir con los tiempos y mantener las esperanzas de un siglo - Una INTERPOL que mira al futuro"*. Discurso presentado en la 86ª reunión de la Asamblea General de INTERPOL, Beijing, China. 26 de septiembre de 2016 (disponible en https://www.interpol.int/es/content/download/5351/file/17Y1721%20S%20DISCURSO%20PRESIDENTE%2086%20REUNION%20AG.pdf; última consulta 27/03/2025).

Meng, H. *"Ir con los tiempos y mantener las esperanzas de un siglo - Una INTERPOL que mira al futuro"*. Discurso en la 86ª reunión de la Asamblea General de INTERPOL, Beijing, China. INTERPOL, 2017 (disponible en https://www.interpol.int/es/content/download/5351/file/17Y1721%20S%20DISCURSO%20PRESIDENTE%2086%20REUNION%20AG.pdf; última consulta en 30/03/2025).

Naciones Unidas. *"Paz, justicia e instituciones sólidas: Objetivo 16"*. Naciones Unidas, s.f., (disponible en https://www.un.org/sustainabledevelopment/es/peace-justice/; última consulta en 05/03/2025).

Oficina de las Naciones Unidas contra la Droga y el Delito. *"Cybercrime in brief*", UNODC, (s.f.) (disponible en https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html; última consulta 20/03/2025).

Oficina de las Naciones Unidas contra la Droga y el Delito. (2024). *"Global Programme on Cybercrime Training Catalogue"*. UNODC, 2024 (disponible en https://www.unodc.org/unodc/en/cybercrime/home.html; última consulta en 20/03/2025).

Oficina de las Naciones Unidas contra la Droga y el Delito. "Ciberdelito", UNODC, s.f. (disponible en https://www.unodc.org/unodc/en/cybercrime/index_new.html; última consulta en 20/03/2025).

Oficina de las Naciones Unidas contra la Droga y el Delito. *"Estados Miembro de las Naciones Unidas aprueban borrador para una convención contra la ciberdelincuencia"*.

UNODC, agosto 2024 (disponible en https://www.unodc.org/lpomex/es/noticias/agosto-2024/estados-miembro-de-las-naciones-unidas-aprueban-borrador-para-una-convencion-contra-la-ciberdelincuencia.html; última consulta en 10/03/2025).

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). *"Estudio exhaustivo sobre el delito cibernético"*. Naciones Unidas, 2013. (disponible en https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf; última consulta en 27/03/2025).

Organización de las Naciones Unidas. *"El sistema de las Naciones Unidas"*. Naciones Unidas, s.f., (disponible en https://www.un.org/es/about-us/un-system; última consulta en 30/05/2025).

Organización de las Naciones Unidas. *"UN Sustainable Development Cooperation Framework Guidance"*, 2019 (disponible en https://unsdg.un.org/sites/default/files/2019-10/ES_UN%20Sustainable%20Development%20Cooperation%20Framework%20Guidance.pdf; última consulta em 20/03/2025).

Pacto Mundial de la ONU España. *"Potencialidades y debilidades del sector de las TIC ante los ODS"*. Pacto Mundial. 5 de diciembre de 2023 (disponible en https://www.pactomundial.org/noticia/potencialidades-y-debilidades-del-sector-de-las-tics-ante-los-ods/; última consulta 27/03/2025)

TechTarget. *"Confidentiality, integrity and availability (CIA)"*, TechTarget, (s.f.) (disponible en https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA; última consulta 27/03/2025).

Uy, I. J. E. *"Foro Económico Mundial, Perspectivas mundiales de ciberseguridad para 2025"* (p. 14), 2025 (disponible en https://es.weforum.org/publications/global-cybersecurity-outlook-2025/; última consulta en 28/03/2025).

UNESCO. *"Internet Governance"*. UNESCO, s.f., (disponible en https://www.unesco.org/es/internet-governance; última consulta en 15/03/2025).

Universidad Internacional de La Rioja (UNIR). *"Principios de seguridad informática"*, UNIR Revista, s.f., (disponible en https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/; última consulta 27/03/2025).

World Economic Forum. *"5 maneras de lograr una resiliencia cibernética efectiva",* noviembre de 2024 (disponible en https://es.weforum.org/stories/2024/11/5-maneras-de-lograr-una-resiliencia-cibernetica-efectiva/; última consulta 28/03/2025).

World Economic Forum. *"Global risks ranked by severity [Infografía]. En Global Risks Report 2025",* World Economic Forum, 2025 (disponible en https://es.weforum.org/publications/global-cybersecurity-outlook-2025/; última consulta en 28/03/2025).

World Economic Forum. *"Informe de Riesgos Globales 2025: Conflictos, medioambiente y desinformación, principales amenazas"*. Foro Económico Mundial, 2025 (disponible en https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/; última consulta en 25/03/2025).

XXXII Seminario Internacional de seguridad y defensa - Amenazas desde el Ciberespacio, Madrid, septiembre de 2020 (disponible en https://repositorio.comillas.edu/xmlui/handle/11531/55854; última consulta en 28/03/2025).

ANEXO I

Abreviaturas y acrónimos

ONU	Organización de las Naciones Unidas
INTERPOL	Organización Internacional de Policía Criminal
TIC	Tecnologías de la información y la comunicación
UNODC	Oficina de Naciones Unidas contra la droga y el delito
Art.	Artículo
MIM	Man in the Middle
OCN	Oficina Central Nacional
CMSI	Cumbre Mundial sobre la Sociedad de la Información
T-CY	Comité de la Convención sobre Delitos Cibernéticos
IA	Inteligencia Artificial
IRTs	Equipos de Respuesta a Incidentes
CNI	Centro Nacional de Inteligencia