



INTERPOL

NOTA INFORMATIVA

SOBRE LAS GARANTÍAS QUE OFRECE EL SISTEMA DE INFORMACIÓN DE INTERPOL PARA EL TRATAMIENTO DE DATOS PERSONALES

RESUMEN

En el presente documento se pretende ofrecer una descripción autorizada de algunos de los principales procedimientos, normas y mecanismos de INTERPOL relativos a la protección de los datos personales en el marco de la cooperación policial y el intercambio de datos con los países miembros de INTERPOL, entre ellos y con socios seleccionados, tales como otras organizaciones internacionales.

En la sección 1 del documento se expone un panorama muy general de la creación de la Organización y una breve descripción del Sistema de Información de INTERPOL. A continuación se explica con más detalle el sistema de notificaciones rojas de INTERPOL. En este apartado se exponen, entre otras cuestiones, los requisitos para la publicación de notificaciones rojas, la revisión previa a la publicación de cada notificación y las circunstancias que conducen a la anulación de notificaciones rojas.

En la sección 2 se presenta un resumen detallado del marco jurídico que subyace a las prácticas de INTERPOL en materia de protección de datos personales y privacidad. Asimismo se describe la amplia experiencia de INTERPOL en el tratamiento y la protección de datos. Se explica cómo, en el marco del Estatuto y del Reglamento de INTERPOL sobre el Tratamiento de Datos (RTD), la Organización trata principios esenciales de la protección de datos como los siguientes: licitud; definición y limitación de la finalidad; calidad de los datos; transparencia; confidencialidad y seguridad de los datos; y supervisión independiente y reparación individual (derechos de acceso individual, rectificación y eliminación), incluidas las normas relativas a la conservación, acceso y transferencia de datos. A continuación se ofrece un resumen detallado de la función de la Comisión de Control de los Ficheros de INTERPOL, su independencia y sus competencias de supervisión y control, que garantizan que este órgano independiente pueda proporcionar un recurso efectivo a los particulares.

Este documento no pretende ofrecer una relación exhaustiva de los mecanismos de protección de datos en INTERPOL, ni sustituir ni matizar en modo alguno las normas y procedimientos vigentes que rigen la cooperación (y que aparecen citados o mencionados en el mismo con frecuencia). Su finalidad es más bien sintetizar y contextualizar algunos de los aspectos más destacados del sofisticado régimen de gestión y protección de datos de la Organización. Para facilitar la consulta, los anexos de este documento contienen recursos fundamentales, tales como el Estatuto y el Reglamento de INTERPOL sobre el Tratamiento de Datos (RTD) de INTERPOL.

INTRODUCCIÓN

En el presente documento se expone un panorama general de la situación de INTERPOL y de sus actividades en cuanto organización internacional creada para facilitar la cooperación de la policía y de las fuerzas del orden a escala internacional, prestando una atención especial a su sistema de notificaciones rojas y a sus reglamentos y prácticas internos en materia de tratamiento y protección de datos personales. En la sección 1 se presenta un cuadro general de la Organización, del Sistema de Información de INTERPOL y de su sistema de notificaciones rojas. En la sección 2 se describen las estructuras jurídica, reglamentaria y operativa para la protección de datos y la privacidad que subyacen a la utilización de dichos sistemas por parte de la Organización y de los países miembros. Los mecanismos jurídicos vinculantes descritos en el presente documento son el eje en torno al cual se articula el compromiso inveterado de INTERPOL con proteger y gestionar los datos de manera segura y efectiva, y, en particular, los datos personales.

SECCIÓN 1: PANORAMA GENERAL DE INTERPOL Y DE SUS SISTEMAS DE INFORMACIÓN Y DE NOTIFICACIONES ROJAS

I. INTERPOL – PRESENTACIÓN GENERAL

La Organización Internacional de Policía Criminal-INTERPOL [en adelante, “INTERPOL”] es una organización internacional constituida con arreglo al derecho internacional público.

Desde su creación en 1923, INTERPOL se ha esforzado por facilitar la cooperación policial internacional. Este mandato está consagrado en el artículo 2 de su Estatuto (aprobado en 1956), en el que se dispone que los fines de la Organización son:

- 1) “conseguir y desarrollar, dentro del marco de las leyes de los diferentes países y del respeto a la Declaración Universal de Derechos Humanos, la más amplia asistencia recíproca de las autoridades de policía criminal;
- 2) establecer y desarrollar todas las instituciones que puedan contribuir a la prevención y a la represión de las infracciones de derecho común.”

INTERPOL, cuya sede está en Lyon (Francia), está integrada por 194 países, cada uno de los cuales designa a una Oficina Central Nacional (OCN). Estas sirven de punto de contacto del país para los asuntos relacionados con INTERPOL y actúan de enlace entre los diversos servicios del país y la Secretaría General de la Organización, así como con las OCN de otros países (artículo 32 del Estatuto).

Las actividades de INTERPOL y el uso que sus Miembros hacen de su Sistema de Información se rigen por el Estatuto y los reglamentos de INTERPOL, en particular el RTD, como se expone en detalle más adelante.

II. EL SISTEMA DE INFORMACIÓN DE INTERPOL

Al proporcionar a sus países miembros acceso a su sistema de comunicación, INTERPOL es la única organización del planeta que facilita una cooperación en asuntos policiales estructurada. De hecho, este intercambio estructurado y regulado de información policial constituye el núcleo del mandato de la Organización, ya que entre sus objetivos estratégicos figura el de servir de centro mundial de información para facilitar la cooperación eficaz entre las fuerzas del orden. La importancia de la red de comunicación y las bases de datos de INTERPOL y las ventajas

de su utilización han sido reconocidas en convenios internacionales y regionales¹ así como en numerosas resoluciones aprobadas por el Consejo de Seguridad y por la Asamblea General de las Naciones Unidas, entre ellas las relacionadas con la lucha contra el terrorismo y la delincuencia organizada transnacional².

III. EL SISTEMA DE NOTIFICACIONES ROJAS DE INTERPOL

Entre las herramientas más importantes de que disponen los Miembros de INTERPOL figura el sistema de notificaciones rojas. Una notificación roja es una solicitud para localizar y detener provisionalmente a una persona, mientras se espera su extradición. Basándose en una orden de detención nacional en vigor, un país miembro puede pedir a la Secretaría General de INTERPOL que publique una notificación roja. Esta puede asimismo publicarse a petición de entidades tales como tribunales internacionales.

Como se ha indicado, la notificación roja se basa en órdenes de detención nacionales expedidas de conformidad con la legislación nacional del país solicitante. Una notificación roja no es una orden de detención internacional. Es competencia absoluta de cada país decidir si solicita la publicación de una notificación roja. INTERPOL no está facultada para dictar órdenes de detención ni publicar notificaciones rojas por iniciativa propia.

Por otra parte, la publicación de una notificación roja no exige a ningún otro país miembro de INTERPOL la adopción de medidas en relación con dicha notificación o con la persona en cuestión. Queda a la discreción de cada Miembro, en función de su propia legislación nacional, actuar sobre la base de notificaciones rojas publicadas a petición de otros países.

Naturalmente, todas las solicitudes de publicación de notificaciones rojas deben cumplir los requisitos establecidos en la legislación nacional del país solicitante y cualesquiera convenios de los que este sea parte. Y hay otra exigencia crucial: todas las solicitudes deben cumplir, además, los requisitos establecidos en el Estatuto y los reglamentos de INTERPOL, en especial en el RTD.

Por ejemplo, para que se publique una notificación roja, la solicitud debe tener por objeto un delito grave de derecho común³. La pena asociada a ese delito debe superar un límite mínimo⁴. La solicitud debe contener suficientes datos de identificación y descripciones del delito⁵. La solicitud no puede presentar un carácter político, militar, religioso o racial, o referirse a delitos políticos, como la traición o el espionaje⁶. Las solicitudes deben cumplir las normas sobre derechos humanos internacionalmente reconocidas que recoge la Declaración Universal de Derechos Humanos (véase el artículo 2(a) del Estatuto). Por ejemplo, de conformidad con la política de INTERPOL en materia de refugiados, no es posible publicar una notificación roja sobre una persona a quien se haya confirmado la condición de refugiado.

1 Por ejemplo: 1) El posible uso del conducto de INTERPOL para transmitir órdenes de detención europeas; 2) el posible uso del conducto de INTERPOL para intercambiar solicitudes de asistencia judicial recíproca se menciona en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) y en la Convención de las Naciones Unidas contra la Corrupción (UNCAC); y 3) en la reciente Convención del Consejo de Europa sobre los Delitos relacionados con Bienes Culturales ("Convención de Nicosia", 2017) se pide a los Estados parte que alimenten la base de datos de INTERPOL sobre obras de arte robadas.

2 Por ejemplo: 1) La resolución 2462 (2019) del Consejo de Seguridad de la ONU alienta a los Estados Miembros de la ONU a que aprovechen al máximo las capacidades policiales de INTERPOL, como las bases de datos y los archivos de análisis pertinentes, a fin de prevenir y reprimir la financiación del terrorismo. 2) La resolución 71/19 de la Asamblea General de la ONU, en la que se pide que se refuerce la cooperación con INTERPOL, especialmente en la lucha contra el terrorismo, la delincuencia transnacional, la ciberdelincuencia, la corrupción y la delincuencia financiera, y los delitos contra el medio ambiente. Para más información sobre las resoluciones de la ONU sobre la Organización, véase el sitio web público de INTERPOL: <https://www.interpol.int/es/Nuestros-interlocutores/Socios-de-organizaciones-internacionales/INTERPOL-y-las-Naciones-Unidas/Resoluciones-de-la-Asamblea-General-y-el-Consejo-de-Seguridad-de-las-Naciones-Unidas-sobre-INTERPOL>.

3 Artículo 83 del RTD.

4 Artículo 83 del RTD.

5 Artículo 83 del RTD.

6 Artículo 3 del Estatuto; artículos 5 y 34 del RTD.

Para garantizar la conformidad con la normativa de INTERPOL y prevenir el uso abusivo del sistema, cada solicitud de publicación de una notificación roja es objeto de un examen independiente e individualizado por parte de la Secretaría General antes de su publicación y difusión a los países miembros de INTERPOL (artículo 86 del RTD). A tal efecto, un grupo especializado multidisciplinar lleva a cabo un riguroso control jurídico y de calidad.

El sistema de notificaciones rojas ha facilitado gran número de detenciones y la extradición de muchas personas que han cometido delitos graves en los países miembros de INTERPOL⁷.

Una vez publicadas, las notificaciones rojas pueden eliminarse de varios modos:

- Cuando la OCN que solicitó su publicación retira la notificación roja.
- Cuando la Secretaría General concluye que la notificación roja no debe mantenerse. Esta conclusión puede basarse en varios motivos⁸, entre ellos que la notificación roja ha dejado de cumplir las condiciones de publicación o las normas establecidas por INTERPOL.
- Cuando la Comisión de Control de los Ficheros de INTERPOL (CCF), órgano independiente de supervisión, concluye que la notificación roja no cumple la normativa de INTERPOL. Tal como se explicará más adelante, tal decisión es definitiva y vinculante para la Organización, y la Secretaría General la aplica inmediatamente⁹.
- A raíz de un procedimiento de resolución de controversias: Con arreglo a la normativa de INTERPOL, un país puede protestar por la publicación de una notificación roja a petición de otro país. Si tal controversia no puede resolverse de mutuo acuerdo, el asunto se someterá al Comité Ejecutivo de INTERPOL, que decidirá si la notificación debe o no mantenerse¹⁰.

Las notificaciones rojas se actualizan periódicamente en función de la información que la OCN solicitante u otras fuentes hacen llegar a la Secretaría General.

Un ejemplo bastante claro puede ser que un país informe de que se ha denegado una solicitud de extradición sobre la persona objeto de una notificación roja. En ese caso, la información se añadirá al expediente de la persona y todos los países miembros podrán consultarla.

Otro ejemplo similar, aunque potencialmente más complejo, es el de la práctica de INTERPOL de añadir ese tipo de notificaciones al expediente de una persona cuando se ha planteado una excepción non bis in idem, principio por el cual no se puede juzgar a una persona dos veces por el mismo delito. En este caso, INTERPOL parte del requisito establecido en el artículo 2 (1) de su Estatuto de respetar la Declaración Universal de Derechos Humanos y, por consiguiente, de actuar dentro del respeto del artículo 14 (7) del Pacto Internacional de Derechos Civiles y Políticos, según el cual: "Nadie podrá ser juzgado ni sancionado por un delito por el cual haya sido ya condenado o absuelto por una sentencia firme de acuerdo con la ley y el procedimiento penal de cada país"¹¹.

Por consiguiente, a fin de respetar la legislación de sus 194 países miembros y sus diversos

7 Algunos casos de detenciones practicadas a partir de notificaciones rojas se detallan en el sitio web público de INTERPOL. Por ejemplo, consúltense los siguientes enlaces: 1) <https://www.interpol.int/News-and-Events/News/2019/Finnish-fugitive-arrested-in-Albania-with-INTERPOL-support>; 2) <https://www.interpol.int/News-and-Events/News/2018/INTERPOL-facial-recognition-nets-most-wanted-murder-fugitive>; 3) <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2018/Una-investigacion-de-INTERPOL-sobre-profugos-permite-detener-a-la-sospechosa-mas-buscada>.

8 En relación con el procedimiento de resolución de controversias, véase el artículo 135 del RTD. En casos excepcionales, el Comité Ejecutivo puede someter la controversia a la Asamblea General. Véase la resolución GA-2017-86-RES-05 de la Asamblea General de INTERPOL.

9 En relación con el procedimiento de resolución de controversias, véase el artículo 135 del RTD. En casos excepcionales, el Comité Ejecutivo puede someter la controversia a la Asamblea General. Véase la resolución GA-2017-86-RES-05 de la Asamblea General de INTERPOL.

10 En relación con el procedimiento de resolución de controversias, véase el artículo 135 del RTD. En casos excepcionales, el Comité Ejecutivo puede someter la controversia a la Asamblea General. Véase la resolución GA-2017-86-RES-05 de la Asamblea General de INTERPOL.

11 Véase el folleto informativo n° 30 de la Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH) de la ONU: "El sistema de tratados de Derechos Humanos de las Naciones Unidas", 3, 6-7. El Pacto Internacional de Derechos Civiles y Políticos ha sido ratificado por 172 Estados miembros.

instrumentos y tratados bilaterales y multilaterales, INTERPOL ha adoptado una práctica que le permite cumplir los requisitos derivados de su Estatuto, y que a continuación se detalla. Por lo general, cuando un país miembro afirma que el principio non bis in idem se aplica a una notificación roja publicada en el Sistema de Información de INTERPOL a petición de otro país, la Secretaría General solicita información adicional a ambos países a fin de realizar una evaluación preliminar sobre la conformidad de los datos con la normativa. Una vez recibida y examinada esa información, si la fuente de los datos (el país que solicita la publicación de la notificación) considera que el principio no se aplica, se opondrá, sobre esa base, a la eliminación de la notificación y confirmará que la persona en cuestión sigue siendo objeto de búsqueda, la Secretaría General añadirá una apostilla a la notificación en la que informará de la posición del país miembro que considera que el principio non bis in idem sí es aplicable. La apostilla servirá para alertar a todos los países miembros de que puede haber motivos para examinar la aplicación del principio non bis in idem a la luz de las leyes nacionales y de los acuerdos internacionales aplicables. Esta práctica preserva, además, el principio de neutralidad de INTERPOL¹².

SECCIÓN 2: MARCO JURÍDICO Y NORMAS DE PROTECCIÓN DE DATOS DE INTERPOL QUE RIGEN EL USO DEL SISTEMA DE INFORMACIÓN DE INTERPOL Y LA PUBLICACIÓN DE NOTIFICACIONES ROJAS

1. DILATADA EXPERIENCIA DE INTERPOL EN PROTECCIÓN DE DATOS

La protección de datos es fundamental para el cometido y las actividades de INTERPOL, y su importancia crucial en el trabajo de la Organización refleja el compromiso de esta con la privacidad de las personas, la gobernanza y el rendimiento de cuentas. Dado que INTERPOL facilita la cooperación y la comunicación entre los organismos encargados de la aplicación de la ley en un entorno de confianza, resulta fundamental que la información intercambiada se ajuste a unas normas sobre protección de datos que son cambiantes.

La importancia que reviste la privacidad de las personas en la actividad de INTERPOL fue reconocida oficialmente ya en 1974, cuando la Asamblea General de la Organización aprobó la resolución que tenía por asunto “Carácter confidencial de la información” (AGN/43/RES1), por la que se instaba a las OCN y a la Secretaría General a que al intercambiar información policial tuvieran en cuenta el respeto de la vida privada de las personas.

Con el objetivo de dar forma a estos compromisos, en 1982 INTERPOL creó un organismo independiente encargado de la protección de datos, poco después de la firma del Convenio 108 del Consejo de Europa¹³, que vino a constituir el primer convenio internacional vinculante en materia de protección de datos. El mandato de este organismo, hoy denominado “Comisión de Control de los Ficheros de INTERPOL” (CCF), fue recogido en el Estatuto de INTERPOL en 2008 y se detalla más adelante.

En 1984 entró en vigor la primera serie de normas de la Organización sobre protección de datos, el denominado “Reglamento relativo a la Cooperación Policial Internacional y al Control Interno de los Ficheros de la OIPC-INTERPOL”.

A fin de proporcionar garantías en un mundo globalizado, digitalizado y en rápida evolución, y con arreglo a las cambiantes normas internacionales sobre protección de datos, INTERPOL

¹² Por lo general, la aplicación del principio non bis in idem se efectúa poniendo en práctica los tratados de extradición existentes entre los Miembros de INTERPOL, y se suele reconocer en relación con el Estado requerido, es decir, la extradición será denegada si la persona en cuestión ya ha sido absuelta o condenada en firme en el Estado requerido por el mismo delito o los mismos delitos. Además, en la práctica la norma no tiene una aplicación única y universalmente aceptada y su interpretación varía según los sistemas jurídicos, y no se aplica de manera generalizada en relación con infracciones de leyes penales cometidas en más de un Estado. Por consiguiente, la práctica de las apostillas adoptada por INTERPOL facilita la aplicación del principio non bis in idem de conformidad con los tratados de extradición pertinentes y con las legislaciones nacionales de sus Miembros.

¹³ Convenio 108 del Consejo de Europa del 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

evalúa¹⁴ y actualiza regularmente sus normas al respecto, aproximadamente una vez cada tres años. Como se indica más adelante, el reglamento actual entró en vigor en julio de 2012 y desde entonces ha sido objeto de una serie de modificaciones sustanciales.

2. GARANTÍAS ADECUADAS EN EL MARCO JURÍDICAMENTE VINCULANTE DE INTERPOL

La relación de INTERPOL con sus países miembros se basa en una cooperación regulada e institucionalizada. Se rige por el derecho público internacional y los textos normativos aprobados por sus propios órganos constitutivos conforme a una jerarquía de mecanismos jurídicamente vinculantes que se aplican a todos los países miembros cuando utilizan los servicios de INTERPOL; entre dichos servicios se encuentra el Sistema de Información de INTERPOL.

Desde el punto de vista de la protección de datos, las normas jurídicamente vinculantes que establecen esas garantías son el Estatuto de INTERPOL, el RTD y el Estatuto de la Comisión de Control de los Ficheros de INTERPOL.

2.1. Estatuto de INTERPOL

El Estatuto de INTERPOL dispone la superestructura que posibilita el funcionamiento de la Organización y la cooperación de sus países miembros. Entre las condiciones y limitaciones fundamentales que impone figuran las siguientes:

- obligación de trabajar dentro del respeto a la Declaración Universal de Derechos Humanos (artículo 2);
- independencia y neutralidad de la Organización, que está sometida a la prohibición de intervenir en “cualquier actividad o intervención de carácter político, militar, religioso o racial” (artículo 3);
- institución y funcionamiento de un órgano de supervisión independiente: la CCF (artículo 36);
- creación de un proceso de reglamentación que faculta a la Asamblea General para decidir sobre la necesidad de fijar normas internas operativas y restricciones (artículo 8 (d)).

Por lo que atañe a la protección de datos y la privacidad, la Asamblea General ha ido aprobando a lo largo de los años diversas normas sobre el tratamiento de datos, incluido el reglamento actual. La aprobación de estas normas requiere una mayoría de dos tercios de los votos de la Asamblea General.

2.2. Garantías y supervisión - Reglamento de INTERPOL sobre el Tratamiento de Datos (RTD) y funcionario encargado de la protección de datos

El actual Reglamento de INTERPOL sobre el Tratamiento de Datos (RTD) fue aprobado por la Asamblea General en 2011 y entró en vigor en julio de 2012. Se aplica a todo tratamiento de datos en el Sistema de Información de INTERPOL, incluido el tratamiento de datos para la publicación y difusión de notificación rojas.

El alcance del RTD es extraordinario, ya que se trata de un instrumento internacional de protección de datos que contiene un total de 135 disposiciones detalladas y es jurídicamente vinculante para 194 países.

Respeto los principios fundamentales de la protección de datos reflejados en distintos

¹⁴ El Comité Permanente de INTERPOL sobre Tratamiento de Datos fue creado en 2019 para garantizar la evaluación continua de las normas de protección de datos aplicables y proponer actualizaciones de las mismas, atendiendo en todo momento a las normas internacionales de protección de datos. El Comité Permanente sustituye al Grupo de Trabajo sobre el Tratamiento de la Información (GTI), constituido en 2002. Además, en el año 2011 la CCF encargó al CRIDS (Centre de Recherche Information, Droit et Société) de la Universidad de Namur (Bélgica) que realizara un estudio sobre el marco de protección de datos de INTERPOL. El estudio concluyó que el marco jurídico que rige el tratamiento de datos de INTERPOL se encuentra entre los más avanzados que el CRIDS ha estudiado.

instrumentos internacionales y regionales, como la licitud, la limitación de la finalidad, la calidad de los datos, la transparencia, la confidencialidad y la seguridad (Título I, Capítulo II). Dispone explícitamente el derecho de acceso, rectificación y eliminación de datos, que se puede ejercer mediante el envío de una solicitud a la CCF (artículo 18).

Define claramente las funciones y responsabilidades de todos los usuarios del Sistema de Información de INTERPOL. Reitera y desarrolla los requisitos de conformidad con las normas, como los dispuestos en los artículos 2 y 3 del Estatuto mencionados anteriormente (artículo 34 del RTD). Cabe destacar que dispone garantías adicionales como la determinación de periodos de conservación de datos (artículos 49 y 50), las restricciones de acceso (artículo 58), y el deber de los usuarios finales de verificar la exactitud y pertinencia de los datos antes de actuar basándose en ellos (artículo 63).

Por lo que toca a las notificaciones, el RTD define las condiciones de publicación de cada tipo de notificación, en particular las rojas (artículos 82-87). Asimismo, detalla la obligación de estudiarlas antes de proceder a su publicación (artículo 77), de garantizar su conformidad con la normativa una vez publicadas (artículo 74), y de eliminar aquellas que ya no cumplan las condiciones dispuestas en los textos normativos (artículo 81).

Habida cuenta de la naturaleza de los datos tratados por conducto de INTERPOL (se trata de datos policiales) y para asegurar el respeto de los derechos de las personas, el RTD define unos grados de confidencialidad que se aplican a los datos tratados e impone requisitos para un acceso limitado a los datos (artículos 112-114). Se ha creado en la Secretaría General una Oficina de Confidencialidad para velar por el cumplimiento de estas disposiciones. Además, este reglamento prevé la gestión del sistema de seguridad estipulando la designación de un servicio de seguridad, la realización de evaluaciones del riesgo y la solución de incidentes relacionados con la seguridad (artículos 115-118 del RTD), entre otras medidas.

En cuanto a las futuras transmisiones de datos, el RTD define también las condiciones para el tratamiento externo de datos con fines policiales: los datos tratados en un principio por el Sistema de Información de INTERPOL pueden ser tratados después fuera de este únicamente si el tratamiento es necesario, se lleva a cabo con fines policiales y cumple los principios al respecto dispuestos en el RTD (artículo 16 (1)). Las OCN que realicen estas operaciones también deberán velar por la aplicación de los requisitos de seguridad y confidencialidad establecidos en el RTD (16 (2)).

Además, la concesión de acceso al sistema de INTERPOL a los organismos nacionales encargados de la aplicación de la ley (denominados en el RTD "entidades nacionales") debe ajustarse a un proceso establecido en el RTD. Entre las obligaciones de las OCN al respecto se encuentra la de garantizar que la entidad nacional esté en condiciones de respetar el RTD, la de firmar un acuerdo con la entidad nacional basado en una Carta sobre el acceso al sistema anexa al RTD, y la de informar a la Secretaría General y a todas las demás OCN de la concesión de derechos de acceso (artículo 21).

En algunos aspectos, el RTD ofrece garantías adicionales que no se hallan necesariamente en otros instrumentos destinados a la protección de datos; por ejemplo, incluye una disposición sobre la "aplicación efectiva" del RTD a través de medidas de control, lo que constituye un nuevo principio de protección de datos (artículo 17).

El principio de "aplicación efectiva" se garantiza, por ejemplo, mediante la inclusión en el RTD de un título completo dedicado a los controles (Título 4). En dicho título se definen los diferentes niveles de control dispuestos y los medios proporcionados para ejercitarlos. Las OCN pueden solicitar información sobre el modo en que una OCN utiliza los datos de los que ellas son fuente (artículo 122 del RTD). Las OCN tienen la obligación de evaluar el funcionamiento de las entidades nacionales a las que han autorizado a acceder directamente al sistema, y de informar a la Secretaría General de las verificaciones de oficio que hayan realizado, los incidentes de seguridad de los que se hayan ocupado y la formación que hayan impartido (artículo 123). A fin de velar por el cumplimiento del RTD, la Secretaría General podrá crear bases de datos de gestión de la conformidad (artículo 125).

Además, con arreglo al Título 4, la Secretaría General debe aplicar medidas cautelares si surge alguna duda sobre la conformidad con el RTD, y para prevenir cualquier daño que los datos pudieran causar a la Organización, los países miembros o las personas a quienes se refieran dichos datos (artículo 129). Estas medidas pueden abarcar, por ejemplo, la suspensión provisional de una notificación roja hasta que se proceda a su examen ulterior. La Secretaría General también está facultada para tomar medidas correctivas destinadas a que el tratamiento de datos se lleve a cabo conforme a la normativa (por ejemplo, corrección de errores de tratamiento, supervisión por la Secretaría General de las operaciones de tratamiento llevadas a cabo por una OCN,

suspensión de los derechos de acceso y tratamiento) (artículo 131) y para pedir a una OCN que imponga medidas correctivas a una entidad nacional, o poner fin al acceso de esta al sistema, en el caso de que la citada entidad trate reiteradamente los datos de manera no conforme con la normativa (artículo 123 (4)).

En cumplimiento de las disposiciones contenidas en ese título, la Secretaría General creó en 2016 una Oficina de Protección de Datos en la Secretaría General (artículo 121A del RTD). Como estipula el artículo 121A del RTD, el funcionario de INTERPOL encargado de la protección de datos ejerce sus funciones con independencia y rinde cuentas directamente al Secretario General. Entre sus funciones cabe destacar la supervisión de la legalidad de los datos tratados en el Sistema de Información de INTERPOL y su conformidad con la normativa; el asesoramiento sobre las operaciones de tratamiento que pueden poner en peligro los derechos y las libertades de las personas, lo que incluye el análisis de las consecuencias del tratamiento en la protección de los datos; la impartición de formación, y la coordinación con la CCF, los funcionarios encargados de la protección de datos en las OCN y otras instituciones y organismos.

En este título se dispone asimismo la necesidad de que los 194 países miembros de la Organización nombren a un funcionario encargado de la protección de datos en sus respectivas OCN; el cometido de estos funcionarios consiste en actuar como guardianes en los puntos extremos del Sistema de Información de INTERPOL. Las OCN también deben nombrar a un funcionario encargado de la seguridad que vele por el respeto de los procedimientos relacionados con la seguridad de la información.

Desde que el RTD fue aprobado se han introducido modificaciones, en 2014 y en 2016. A fin de garantizar que el marco jurídico de INTERPOL siga reflejando los cambios que se producen sobre el terreno desde numerosas perspectivas operacionales, entre ellas la de la protección de datos, en 2018 la Asamblea General encomendó a un grupo de trabajo especial integrado por representantes de los países miembros de INTERPOL que revisara el RTD y propusiera los cambios adicionales que fueran necesarios. La Asamblea General aprobó en su reunión de octubre de 2019 las diversas modificaciones propuestas.

2.3. Supervisión y medidas que pueden adoptarse – Estatuto de la Comisión de Control de los Ficheros de INTERPOL

Como se ha indicado anteriormente, la Comisión de Control de los Ficheros de INTERPOL (CCF) es un órgano independiente e imparcial que fue creado en 1982 con el cometido de garantizar que el tratamiento de datos personales por parte de INTERPOL se lleve a cabo de acuerdo con las normas de la Organización.

Este órgano dispone de mecanismos de recurso para los afectados por el tratamiento de datos. Con los años, la función de la CCF se ha visto fortalecida. Por ejemplo, en 2003, con ocasión de la Conferencia Internacional de Comisarios para la Protección de Datos y la Privacidad, fue acreditada y reconocida como autoridad en materia de protección de datos, y en 2008 se incluyó la descripción de sus funciones y su mandato en el Estatuto de INTERPOL.

En 2016, la Asamblea General de INTERPOL aprobó un nuevo marco jurídico aplicable a la CCF. El nuevo Estatuto de la CCF, que entró en vigor en marzo de 2017, refuerza la situación y las capacidades de la CCF para desempeñar sus funciones.

De conformidad con su propio Estatuto, la CCF está compuesta de dos cámaras:

1) La Cámara de Supervisión y Asesoramiento, que es competente para llevar a cabo las verificaciones necesarias para garantizar la conformidad con las normas de INTERPOL, y con este fin puede emitir decisiones vinculantes para la Organización sobre las medidas necesarias para subsanar todo incumplimiento de las normas (artículo 26 (1)). También emite dictámenes sobre todo asunto relacionado con el tratamiento de los datos de carácter personal (artículo 26 (2)). Por ejemplo, el RTD dispone la obligación de solicitar el dictamen de la CCF antes de crear una base de datos que contenga información de carácter personal o de firmar con otra entidad un acuerdo que implique el intercambio de datos personales.

2) La Cámara de Solicitudes, que tiene la competencia exclusiva de examinar las solicitudes presentadas por particulares de acceso, rectificación o eliminación de datos tratados en el Sistema de Información de INTERPOL, y tomar decisiones al respecto (artículo 28 (1, b)).

La Cámara de Solicitudes, que tiene la competencia exclusiva de examinar las solicitudes presentadas por particulares de acceso, rectificación o eliminación de datos tratados en el Sistema de Información de INTERPOL, y tomar decisiones al respecto (artículo 28 (1, b)) **recurso efectivo** a las personas fundándose en los principios sentados en la jurisprudencia, especialmente la del Tribunal Europeo de Derechos Humanos (véase el caso Waite y Kennedy). Concretamente, se cumplen los siguientes criterios:

- **Accesibilidad directa:** Las personas pueden enviar sus solicitudes a la CCF de manera directa y gratuita (artículo 18 del RTD; artículos 29 y 30 (3) del Estatuto de la CCF), y estas solicitudes tienen carácter confidencial (artículo 20 (2) del Estatuto de la CCF; normas 13 y 29 de las Normas de Funcionamiento de la CCF).
- **Independencia e imparcialidad:** El Estatuto de la CCF refuerza la independencia de la CCF dispuesta en el artículo 36 del Estatuto de INTERPOL (artículos 4, 5 (1), 11, 15 (4) del Estatuto de la CCF), su imparcialidad y la de sus miembros (artículos 12 y 13 del Estatuto de la CCF).
- **Experiencia y conocimientos especializados:** Los miembros de la CCF son expertos en las materias pertinentes, como se exige para órganos similares (por ejemplo, experto en protección de datos, experto en derechos humanos, etc.) (artículo 8 del Estatuto de la CCF).
- **Acceso libre y sin reservas:** La CCF goza de un derecho de acceso libre y sin reservas a todos los datos tratados en el Sistema de Información de INTERPOL (artículo 19 del Estatuto de la CCF).
- **Igualdad de armas:** El Estatuto de la CCF garantiza la igualdad de armas entre la persona y el país que trató sus datos; por ejemplo, en la comunicación de la información (artículo 35 del Estatuto de la CCF), y en el hecho de que las decisiones adoptadas son vinculantes para todas las partes (artículo 38 (1) del Estatuto de la CCF).
- **Regulación temporal del procedimiento:** En el Estatuto de la CCF se han introducido plazos concretos para las actuaciones del procedimiento (artículos 31(1), 32(1), 40 y 41).
- **Decisiones vinculantes/definitivas/motivadas:** Las decisiones de la CCF son definitivas y vinculantes para la Organización (artículo 38 (1) del Estatuto de la CCF). De conformidad con el Estatuto de la CCF, las decisiones deben motivarse (artículo 38 (2)). A reserva de los requisitos de confidencialidad, algunas decisiones se publican en el sitio web de INTERPOL, en <https://www.interpol.int/es/Quienes-somos/Comision-de-Control-de-los-Ficheros-de-INTERPOL-CCF/Reuniones-e-informes-de-la-CCF> (artículo 44 del Estatuto de la CCF; sitio web de INTERPOL). Aunque las decisiones de la CCF sean definitivas, se pueden enviar solicitudes de revisión si se cumplen ciertas condiciones (artículo 42 del Estatuto de la CCF).
- **Medidas que pueden adoptarse:** La CCF está facultada para decidir la adopción de medidas adecuadas a las que puedan recurrir las personas (artículo 39 del Estatuto de la CCF).

3. ALCANCE GLOBAL DEL PAPEL DESEMPEÑADO POR INTERPOL EN EL FOMENTO DE LAS NORMAS DE PROTECCIÓN DE DATOS

Con su conjunto excepcional de normas vinculantes en materia de protección de datos, y sus correspondientes medidas de aplicación, INTERPOL contribuye a aumentar el nivel de protección de datos en todo el mundo a través de sus 194 países miembros.

Una de las medidas clave emprendidas por INTERPOL para asegurarse de que su marco jurídico está debidamente adaptado es mantenerse informada en todo momento de las últimas

novedades relativas a las normas y prácticas en materia de protección de datos. Esta labor queda reflejada, por ejemplo, en las recomendaciones hechas en las Conferencias Regionales de INTERPOL -que son órganos subsidiarios de la Asamblea General-, las cuales instan a los países miembros de INTERPOL a seguir de cerca las novedades legislativas en materia de protección de datos¹⁵, a tener en cuenta la necesidad de fomentar la promulgación de leyes nacionales sobre protección de datos en el sector policial, y a elaborar y poner en marcha in situ las prácticas de protección adecuadas.

Además, los Jefes de OCN han reconocido la necesidad de “normas estrictas de protección de datos” y les han animado a continuar ampliando la red de funcionarios encargados de la protección de datos en las OCN obligatoriamente designados de conformidad con el RTD. Esta red es única, ya que actualmente ninguna otra organización internacional reúne una red verdaderamente mundial de funcionarios encargados de la protección de datos en el ámbito de la aplicación de la ley. Para reforzar esta red, los funcionarios encargados de la protección de datos en las OCN reciben formación periódica sobre las reglas y normas en la materia¹⁶, participan en conferencias organizadas por la Secretaría General¹⁷, y presentan a la Secretaría General informes anuales sobre las operaciones de tratamiento de datos.

Las prácticas cabales de INTERPOL en materia de protección de datos garantizan la confianza mutua para el intercambio de datos policiales y también ayudan a ofrecer unas capacidades policiales innovadoras. Las soluciones diseñadas por INTERPOL incorporan el principio de “privacidad y protección de datos desde el diseño”, a fin de proteger los derechos de las personas en la creación de herramientas y sistemas que sirven para mantener funciones clave y preservar la eficacia del intercambio de datos¹⁸.

CONCLUSIÓN

INTERPOL es una organización internacional constituida con arreglo al derecho público internacional y cuenta con una prolongada experiencia en tratamiento y protección de datos, así como en fomento de la privacidad. Su marco jurídico, que está basado en una cooperación institucionalizada y regulada y es aplicable a todos sus países miembros, se ha fortalecido a lo largo de décadas y se ha convertido en un completo código de normas vinculantes: el Reglamento de INTERPOL sobre el Tratamiento de Datos, que consagra la “aplicación efectiva” como un principio fundamental de la protección de datos.

A través de sus procedimientos y sus decisiones definitivas y vinculantes, la Comisión de Control de los Ficheros de INTERPOL, órgano de supervisión independiente de la Organización, proporciona un recurso efectivo a las personas objeto de los datos.

El marco jurídico moderno y riguroso de INTERPOL que rige el tratamiento de datos permite a la Organización firmar acuerdos de intercambio de datos con entidades como otras entidades pertinentes, como los órganos jurisdiccionales internacionales.

Al aplicar el Reglamento sobre el Tratamiento de Datos, INTERPOL fomenta y mejora en todo el mundo las normas y garantías en materia de protección de datos.

15 Algunos ejemplos son la evolución de la legislación regional en materia de protección de datos, como el Reglamento General de Protección de Datos (RGPD) y la Directiva sobre protección de datos en el ámbito penal, ambos textos de la Unión Europea.

16 La formación consta de clases presenciales, seminarios web hechos a medida y el acceso a material didáctico y a los documentos pertinentes a través del panel de mandos de las OCN. El curso obligatorio para los funcionarios encargados de la protección de datos va seguido de un curso opcional de perfeccionamiento para instructores (formación de formadores), cuya duración es de cinco días.

17 La primera Conferencia de funcionarios encargados de la protección de datos en las oficinas centrales nacionales (OCN) tuvo lugar en Lyon en octubre de 2018 y se celebrará periódicamente.

18 Entre tales soluciones cabe citar, por ejemplo, el sistema de cifrado de tipo hash utilizado para efectuar comparaciones con imágenes ya presentes en la Base de Datos Internacional de INTERPOL sobre Explotación Sexual de Niños. La utilización de una función criptográfica hash para comparar datos permite tratar eficazmente incluso los datos más delicados, y al mismo tiempo proteger los derechos y la privacidad de las personas interesadas.

Documentos jurídicos:

- Los documentos que rigen las prácticas de INTERPOL en materia de protección de datos son los que se citan a continuación:
- el Estatuto de INTERPOL
- el Reglamento de INTERPOL sobre el Tratamiento de Datos
- el Estatuto de la Comisión de Control de los Ficheros de INTERPOL
- las Normas de Funcionamiento de la Comisión de Control de los Ficheros de INTERPOL

Se pueden consultar en los enlaces siguientes:

can be found at the following links:

1) <https://www.interpol.int/es/Quienes-somos/Marco-juridico/Documentos-juridicos>

2) <https://www.interpol.int/es/Quienes-somos/Comision-de-Control-de-los-Ficheros-de-INTERPOL-CCF/La-CCF>.