2026

DOCUMENTO DE ANTECEDENTES

Tema: "Evaluar el uso indebido y la apropiación internacional de datos personales por parte de corporaciones tecnológicas."

INTERPOL

Moderador y mesa
Angélica Estrada Gudiño y Emiliano Medina Martínez

ÍNDICE

Antecedentes del comité

La Organización Internacional de Policía Criminal (INTERPOL), fundada en 1923, es el organismo especializado de las Naciones Unidas encargado de la cooperación policial para prevenir y combatir la delincuencia internacional. Guiada por su constitución, INTERPOL promueve la colaboración entre las fuerzas del orden para combatir la delincuencia respetando los derechos humanos y la soberanía de los estados miembros.

La INTERPOL facilita el intercambio y el acceso a la información sobre delitos y delincuentes. Además, de que brinda apoyo técnico y operativo para que las autoridades nacionales combatan eficazmente la delincuencia transnacional.

https://www.interpol.int/es/Delitos/Ciberdelincuencia

Introducción del tema

En la actualidad, el uso de la tecnología podría considerarse como uno de los avances más significativos en la historia humana, ya que ha permitido un acceso amplio a la información y ha facilitado la comunicación entre personas de distintas partes del mundo. Sin embargo, este progreso también ha traído consigo diversos desafíos, entre los que destacaría el posible incremento del robo y uso indebido de datos personales. En los últimos años, este tipo de delitos habría tenido un aumento de aproximadamente un 16,9 %, lo que podría implicar que millones de datos personales estén siendo utilizados con fines ilícitos o posiblemente poco éticos.

El crecimiento en el uso indebido y la apropiación de datos personales podría haber generado un entorno en el que ciertas corporaciones tecnológicas tengan la capacidad de emplear esta información de manera cuestionable. Asimismo, podría existir la posibilidad de que dichos datos sean compartidos o comercializados con otras instituciones del mismo rubro, lo que plantea preocupaciones en términos éticos, legales y de derechos humanos.

En este contexto, el principal desafío parecería centrarse en encontrar un equilibrio entre el aprovechamiento de la información y los intereses de las corporaciones tecnológicas. Esta situación habría dado lugar a debates internacionales sobre cómo regular de manera más efectiva el uso y la apropiación de los datos personales, con el objetivo de garantizar la seguridad a nivel global.

Evolución del tema

El uso masivo de datos personales por parte de corporaciones tecnológicas se intensificó con la expansión global de plataformas digitales a partir de la década de los 2000. La creciente interconexión digital permitió una recolección y almacenamiento de información sin precedentes, lo que, paralelamente, generó nuevas vulnerabilidades susceptibles de explotación criminal. Desde 2010, el avance del almacenamiento en la nube, la inteligencia artificial y los servicios digitales transfronterizos incrementó tanto el volumen como la sensibilidad de los datos recopilados.

Las brechas de seguridad en grandes corporaciones han derivado en filtraciones masivas que afectan simultáneamente a múltiples países. En numerosos casos, la información sustraída ha sido utilizada para la comisión de delitos como fraude financiero, robo de identidad, extorsión digital y otras formas de ciberdelincuencia organizada. La naturaleza transnacional del ecosistema digital ha complejizado la investigación penal de estos delitos. Los datos pueden ser recolectados en un Estado, almacenados en otro, comercializados en un tercero y utilizados para victimizar personas en distintas jurisdicciones. Esta fragmentación plantea desafíos significativos en materia de competencia legal, cooperación judicial y coordinación operativa entre autoridades nacionales.

En este contexto, el fortalecimiento de la cooperación policial internacional resulta esencial para prevenir, investigar y desmantelar redes dedicadas al tráfico y uso ilícito de datos personales. La coordinación en el intercambio de inteligencia, el desarrollo de capacidades técnicas y la acción conjunta frente a estructuras de ciberdelincuencia organizada se posicionan como elementos centrales dentro del mandato operativo de INTERPOL frente a esta problemática emergente.

Acciones externas

INTERPOL ha establecido acuerdos de cooperación con organizaciones internacionales, gobiernos nacionales, entidades privadas y organismos regionales para garantizar que el intercambio de datos personales se realice bajo estándares éticos y jurídicos comunes. Estos acuerdos permiten coordinar investigaciones transfronterizas sobre delitos informáticos, incluyendo la apropiación ilícita de datos por parte de empresas tecnológicas. En colaboración con Naciones Unidas y otras entidades multilaterales, INTERPOL promueve el respeto a la soberanía digital de los Estados y apoya la armonización de leyes de protección de datos para cerrar vacíos legales que permiten el abuso corporativo.

INTERPOL ha participado en proyectos jurídicos sobre tecnologías de la información y la comunicación (TIC), enfocados en establecer principios de protección de datos aplicables a nivel global. Estos proyectos han contribuido a definir estándares sobre el tratamiento de datos personales en contextos internacionales, incluyendo el uso de plataformas digitales por parte de corporaciones. Además, INTERPOL ha colaborado en iniciativas para mejorar la trazabilidad de datos y la rendición de cuentas de actores privados, fomentando la transparencia en el uso de información personal y apoyando a los Estados miembros en la persecución de delitos relacionados con la privacidad digital.

Enfoque del comité

El Consejo de Policía Criminal se centra en la solución de problemas en la seguridad nacional en el término tecnológico. Las prioridades del comité incluyen las medidas de seguridad, las precauciones de seguridad llevadas a cabo durante el problema, la acción política, la búsqueda de soluciones ante el problema.

El consejo de Policía Criminal se centra en cuestiones relacionadas con la seguridad internacional, con la facultadde autorizar resoluciones, sanciones, apoyo investigativo e equipos de apoyo. Su propósito es encontrar una solución sobre la apropiación de datos personales. Este comité anima a los delegados a reflexionar sobre la apropiación de los datos personales a nivel mundial, y a desarrollar una compresión más profunda del uso de los datos personales.

ASPECTOS CLAVE PARA DEBATIR:
- Violaciones de los derechos humanos
- Apropiación de los datos personales
- Aspectos éticos sobre el robo de datos personales
- Tensiones entre países involucrados

Conclusión

INTERPOL ha implementado medidas estratégicas para combatir el uso indebido de datos personales por parte de corporaciones tecnológicas, centrando sus esfuerzos en la cooperación internacional y el fortalecimiento de marcos jurídicos globales. Ha establecido acuerdos con organismos internacionales, gobiernos, entidades privadas y regionales para asegurar que el intercambio de datos se realice bajo normas éticas y legales comunes, facilitando así investigaciones transfronterizas sobre delitos informáticos. En colaboración con Naciones Unidas, promueve la soberanía digital de los Estados y la armonización de leyes de protección de datos para cerrar vacíos legales. Además, ha participado en proyectos jurídicos sobre TIC que definen principios globales de protección de datos, y ha impulsado iniciativas para mejorar la trazabilidad y la rendición de cuentas de actores privados, fomentando la transparencia y apoyando a los Estados miembros en la lucha contra delitos que afectan la privacidad digital.

Posición de los países

Reino Unido: Tras el Brexit, el Reino Unido ha reformulado su marco legal con la Ley de Uso y Acceso a los Datos de 2025, buscando equilibrar innovación con protección de derechos. Aunque promueve el intercambio seguro de datos entre sectores, ha recibido críticas por reducir garantías frente al uso gubernamental de información personal.

México: México aplica la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y ha multado a empresas privadas por vulneraciones graves. En 2023, el INAI impuso sanciones por más de 73 millones de pesos. El país busca fortalecer su marco legal ante el crecimiento del comercio digital y el uso corporativo de datos.

Francia: Francia es líder europeo en sanciones contra corporaciones tecnológicas por uso indebido de datos. La CNIL ha multado a empresas como Google y Shein por violar normas de consentimiento y publicidad digital. Además, su Ley para una República Digital refuerza el derecho al olvido y la protección de menores.

Noruega: Aunque no forma parte de la UE, Noruega aplica el RGPD a través del Espacio Económico Europeo. Su autoridad de protección de datos (Datatilsynet) ha sancionado a entidades por uso ilegal de píxeles de rastreo y tratamiento sin base jurídica. El país mantiene una postura firme en defensa de la privacidad digital.

Japón: Japón cuenta con la Ley de Protección de Información Personal (APPI), vigente desde 2003 y actualizada periódicamente. Exige consentimiento explícito para el uso de datos y prohíbe su reutilización sin autorización. Aunque ha mejorado su marco legal, aún enfrenta desafíos en ciberseguridad y supervisión empresarial.

Israel: Israel implementó en 2025 la Enmienda 13, su mayor reforma en 40 años, que endurece el consentimiento, amplía la definición de datos sensibles y permite demandas individuales sin prueba de daño. Sin embargo, ha sido criticado por el uso estatal de tecnología para vigilancia masiva, como reveló Microsoft en 2025.

Posición de los países

Alemania: Alemania es uno de los países con legislación más estricta en protección de datos, liderando la implementación del Reglamento General de Protección de Datos (GDPR) en la Unión Europea. Ha sancionado a empresas como Vodafone por violaciones de privacidad y ha exigido la retirada de apps que transfieren datos sin consentimiento. Su postura es firme en exigir transparencia y responsabilidad corporativa.

Rusia: Rusia exige que los datos personales de sus ciudadanos se almacenen en servidores dentro del país, según su ley de localización de datos desde 2015. Ha multado a empresas extranjeras como Pinterest y Airbnb por incumplir esta normaDPL News. Aunque promueve la soberanía digital, su enfoque ha sido criticado por permitir vigilancia estatal y limitar la transparencia.

China: China aprobó en 2021 la Ley de Protección de Información Personal (PIPL), que exige consentimiento explícito para la recolección de datos. Sin embargo, el Estado mantiene amplias facultades para recopilar información con fines de seguridad nacionalCiberseguridad LATAM. Aunque regula a sus corporaciones, enfrenta críticas por prácticas de vigilancia masiva y falta de garantías individuales.

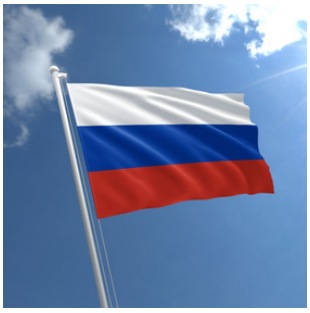
Canadá: Canadá cuenta con la Ley PIPEDA, que regula el uso de datos personales en el sector privado desde el año 2000. En 2022 presentó una nueva ley para dar mayor control a los ciudadanos y sancionar a plataformas digitales que incumplanRadio-Canada. Ha iniciado investigaciones contra empresas como X (Twitter) por uso indebido de datos en entrenamiento de IA.

Estados Unidos: Estados Unidos carece de una ley federal única de protección de datos, aunque varios estados como California han adoptado normas avanzadas. En 2024 se propuso la American Privacy Rights Act (APRA), que busca limitar el poder de las grandes tecnológicas y regular la industria de intermediación de datos. El país enfrenta tensiones con la UE por diferencias regulatorias

Lista de participantes

Alemania

Francia



Rusia

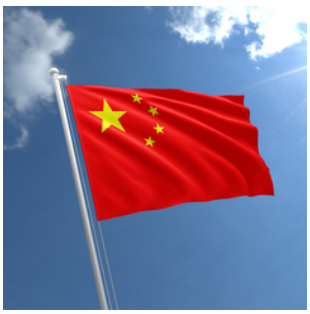
Reino Unido

Estados Unidos

Canadá

Corea del Sur

México



China

India

Brasil

Grecia

Lista de participantes

España

Indonesia

Argentina

Italia

Noruega

Japón

Turquía

Nigeria

Australia

Israel

Referencias

- Adaptación RGPD. (s.f.). La impunidad de los gigantes tecnológicos para exprimir los datos personales. Adaptación RGPD. https://www.adaptacion-rgpd.eu/la-impunidad-de-los-gigantes-tecnologicos-para-exprimir-los-datos-personales/

- INTERPOL. (s.f.). How our history started. INTERPOL. https://www.interpol.int/Who-we-are/Our-history/How-our-history-started

- INTERPOL. (s.f.). Protección de datos. INTERPOL. https://www.interpol.int/es/Quienes-somos/Marco-juridico/Proteccion-de-datos

- INTERPOL. (s.f.). Qué es INTERPOL. INTERPOL. https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL2

- LHH. (2024, agosto 28). Ética y privacidad de datos en el panorama tecnológico actual. LHH Insights. https://www.lhh.com/es/es/insights/etica-y-privacidad-de-datos/

- London Loves Tech. (2024, abril 3). The average data breach cost in the industrial sector surged by $860,000 year-over-year. London Loves Tech. https://londonlovestech.com/the-average-data-breach-cost-in-the-industrial-sector-surged-by-860000-year-over-year/

- SSIR México. (s.f.). Privacidad digital: cómo los gobiernos y empresas abusan de nuestros datos. SSIR México. https://ssires.tec.mx/es/noticia/privacidad-digital-como-los-gobiernos-y-empresas-abusan-de-nuestros-datos

- The Conversation. (2024, abril 4). ¿Está en peligro la impunidad de los gigantes tecnológicos por exprimir nuestros datos personales?. The Conversation. https://theconversation.com/esta-en-peligro-la-impunidad-de-los-gigantes-tecnologicos-por-exprimir-nuestros-datos-personales-202063