Naciones Unidas A/79/173

Asamblea General

Distr. general
17 de julio de 2024

Original: español

Septuagésimo noveno período de sesiones
Tema 71 b) del programa provisional*
Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales

Derecho a la privacidad

Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe preparado por la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères, presentado de conformidad con la resolución 28/16 del Consejo.

* A/79/150.

Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères

Propuesta de actualización de la resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, titulada “Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales”

Resumen

En este informe se presenta una propuesta de actualización de la resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, titulada “Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales” con el propósito de poner al día su contenido para que se ajuste a la realidad socio-tecnológica del siglo XXI.

I. Antecedentes y justificación

1. En la Carta de las Naciones Unidas, suscrita el 26 de junio de 1945[1], se estableció como uno de los propósitos de la Organización el de "realizar la cooperación internacional (…) en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión"[2]. Por consiguiente, los derechos de las personas relativos al tratamiento de sus datos personales también figuran entre los cometidos de la Organización.

2. En efecto, la Asamblea General[3], en su resolución 45/95, de 14 de diciembre de 1990, aprobó los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales"[4]. La resolución fue precedida de las resoluciones 1990/42 de la Comisión de Derechos Humanos, de 6 de marzo de 1990, y 1990/38 del Consejo Económico y Social, de 25 de mayo de 1990, titulada "Principios rectores sobre la utilización de ficheros computarizados de datos personales". Esos principios rectores no son jurídicamente vinculantes para los Estados, pero han sido muy importantes y han sido tenidos en cuenta por los Gobiernos en sus regulaciones internas y citados por jueces y académicos.

3. La resolución 45/95 fue aprobada en 1990 para dar respuestas a las realidades socio-tecnológicas de esa época. Desde entonces han surgido nuevos fenómenos y se han producido avances tecnológicos que han transformado nuestra sociedad y que forman parte de nuestra vida cotidiana. A título de ejemplo, se destacan los siguientes:

- El surgimiento y la popularización de Internet revolucionó la forma en que accedemos a información de todas partes del mundo y la compartimos;
- Los teléfonos inteligentes se han convertido en dispositivos esenciales para la comunicación, el trabajo, la educación y el entretenimiento;
- Las redes sociales digitales han transformado la comunicación y la conexión social en línea;
- La computación en la nube ha modificado la forma en que las empresas y los individuos gestionan la información porque les permite acceder a datos y aplicaciones en línea de todo el mundo y desde cualquier parte del mundo y almacenarlos;
- Los macrodatos han permitido realizar análisis sofisticados y adoptar decisiones sobre la base del procesamiento de grandes cantidades de datos;

[1] El texto oficial de la Carta de las Naciones Unidas puede consultarse en la página web de la Organización: https://www.un.org/es/about-us/un-charter.

[2] Véase el Artículo 1, párrafo 3, de la Carta de las Naciones Unidas. Otros de los propósitos de las Naciones Unidas que se enuncian en ese artículo son los siguientes: "1. Mantener la paz y la seguridad internacionales (…). 2. Fomentar entre las naciones relaciones de amistad basadas en el respeto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, y tomar otras medidas adecuadas para fortalecer la paz universal. 3. Realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión; y 4. Servir de centro que armonice los esfuerzos de las naciones por alcanzar estos propósitos comunes".

[3] La Asamblea General es el órgano principal de las Naciones Unidas de deliberación, adopción de políticas y representación (http://www.un.org/es/ga/).

[4] Los principios se aplican a los ficheros computadorizados de entidades públicas y privadas. También pueden aplicarse, con ciertas adaptaciones, a los ficheros manuales (Véase el párrafo 10 de los principios rectores).

- La inteligencia artificial está generando enormes expectativas y cambios al utilizar algoritmos avanzados y producir información;
- La Internet de las cosas permite interconectar dispositivos físicos a través de Internet y compartir información para automatizar y controlar diversos sistemas a distancia;
- La realidad virtual y la realidad aumentada han permitido crear nuevas experiencias digitales, desde juegos hasta aplicaciones destinadas a la capacitación y simulaciones;
- Los vehículos autónomos, para los que se aprovechan los avances que se han producido en el ámbito de la inteligencia artificial y los sensores que se utilizan para que los automóviles puedan operar con autonomía, han transformado la industria del transporte y la forma en que se trasladan las personas;
- Las neurotecnologías permiten conocer minuciosamente el cerebro y obtener información neuronal de las personas (datos extremadamente sensibles).

4. Ninguno de estos avances tecnológicos se había producido cuando se aprobó la resolución 45/95 de la Asamblea General. Por eso, es necesario actualizarlos para ajustarlos a la realidad socio-tecnológica del siglo XXI. Además, las tecnologías actuales permiten recolectar, desde cualquier parte del mundo, datos de personas domiciliadas o residentes en otros países. Este fenómeno, denominado "recolección internacional de datos"[5] no se contempla en el texto de la resolución a la que se refiere el presente informe y, por ser la forma más utilizada para recolectar datos de personas de todas partes del mundo, debería incorporarse en los documentos internacionales.

5. Por otra parte, la información es esencial para el funcionamiento de las herramientas tecnológicas, como la inteligencia artificial, porque un algoritmo no puede por sí solo producir un resultado, sino que este es consecuencia del procesamiento y análisis de información.

6. Dentro de la información en general, se encuentran los datos personales en particular. Estos son tan valiosos que han sido llamados la "moneda de la economía digital". En este sentido, por ejemplo, a finales de diciembre de 2022, la Organización de Cooperación y Desarrollo Económicos (OCDE) aprobó la declaración sobre un futuro digital fiable, sostenible e inclusivo[6] en la cual se resaltan, entre otras cosas "las conclusiones del proyecto horizontal de la OCDE sobre gobernanza de datos para el crecimiento y el bienestar (…), que reconocen la importancia de los datos como **motor de la economía mundial**" (sin énfasis en el original).

7. Esa organización se comprometió a trabajar, entre otras cosas, para "impulsar una transformación digital centrada en el ser humano y que promueva los derechos humanos, tanto en línea como fuera de ella, así como una sólida protección de los datos personales, leyes y normativas adecuadas a la era digital, y un uso fiable, seguro, responsable y sostenible de las tecnologías digitales emergentes y la inteligencia artificial"[7].

8. El Parlamento Europeo y el Consejo y la Comisión de la Unión Europea, por su parte, aprobaron el 23 de enero de 2023 la Declaración Europea sobre los Derechos y

[5] Nelson Remolina Angarita, *Recolección internacional de datos: un reto del mundo post-internet*, Primera edición (Madrid, España, Agencia Estatal Boletín Oficial del Estado, 2015).

[6] OCDE, "Declaration on a Trusted, Sustainable and Inclusive Digital Future". La declaración fue el resultado de la reunión que se realizó en la Isla Gran Canaria (España), los días 14 y 15 de diciembre de 2022. El texto oficial puede consultarse en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488.

[7] *Ibid.*

Principios Digitales para la Década Digital[8]. En el capítulo III de esa declaración, titulado “Libertad de elección”, y bajo el subtítulo “Un entorno digital justo”, se comprometieron, entre otras cosas, a lo siguiente: “velar por un entorno digital seguro y protegido, basado en la competencia leal, en el que los derechos fundamentales estén protegidos, los derechos de los usuarios y la protección de los consumidores en el mercado único digital estén garantizados y las responsabilidades de las plataformas, especialmente los grandes operadores y los guardianes de acceso, estén bien definidas”.

9. Los acontecimientos señalados han generado, en todo el mundo, la revisión de documentos internacionales pertinentes al tratamiento de datos, así como de leyes locales, con miras a actualizarlos. En este sentido, la Asamblea Global de Privacidad (GPA) aprobó en octubre de 2023 una resolución para alcanzar estándares globales de protección de datos, en la que figuran principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo[9], mediante la cual la GPA insiste en una idea que sostiene desde hace décadas: el objetivo de contar con normas globales sobre protección de datos y privacidad. Para ello, promovió en la declaración algunos principios, derechos y otros elementos importantes para lograr altos niveles de protección de datos y privacidad. En ese documento, la GPA resolvió abogar por los principios, derechos y otros elementos establecidos en esa resolución, promulgarlos y promoverlos para garantizar que puedan implementarse y aplicarse efectivamente en todos los contextos, en particular en el procesamiento de datos con tecnologías e innovaciones nuevas y emergentes.

10. En esa resolución, la GPA enfatizó la importancia de proteger los datos personales a través de fronteras con una variedad de mecanismos de transferencia, como la adecuación, las cláusulas modelo, las certificaciones y los acuerdos administrativos, para garantizar la protección de los datos “viaje” con la información cuando esta circula a través de las fronteras. Asimismo, destacó los beneficios de aprovechar los puntos comunes, las complementariedades y los elementos de convergencia para fomentar la interoperabilidad futura entre los enfoques y mecanismos regulatorios existentes que permitan flujos de datos transfronterizos seguros y confiables[10].

11. Durante el siglo XX se inició un proceso de armonización regulatoria internacional cuyos principales protagonistas han sido el Consejo de Europa, la OCDE, las Naciones Unidas, el Parlamento Europeo y el Consejo de la Unión Europea. En el siglo XXI se sumaron a ese proceso el Foro de Cooperación Económica de Asia y el Pacífico (APEC), la Red Iberoamericana de Protección de Datos y la GPA (anteriormente llamada “Conferencia Internacional de Autoridades de Protección de Datos y Privacidad”).

12. En consonancia con lo señalado, la Red Iberoamericana de Protección de Datos ha manifestado que el “establecimiento de un marco armonizado de protección de datos a nivel global ha sido el principal fundamento de la adopción de los distintos instrumentos internacionales actualmente existentes en materia de protección de datos. Se trata así de garantizar que el desarrollo del comercio a nivel mundial resulte

[8] Parlamento Europeo, el Consejo y la Comisión, Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01), 23 de enero de 2023. El texto oficial puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AJOC_2023_023_R_0001.

[9] Asamblea Global de Privacidad (GPA), resolución “Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide”, octubre de 2023. El texto puede consultarse en: https://globalprivacyassembly.org/document-archive/adopted-resolutions/.

[10] *Ibid.*

compatible con la protección de los derechos de las personas, especialmente en lo que se refiere a la protección de la información que les concierne”[11].

13. Finalmente, resulta necesario hacer referencia al ciberespacio como el escenario en que convivimos millones de personas en el mundo.

14. Los datos personales circulan diariamente en ese “ciberespacio”. No obstante, la regulación sobre el tratamiento de datos surgió en un escenario en el que aún no se hablaba de él. En otras palabras, la realidad socio-tecnológica actual no era la que existía cuando se emitieron las primeras regulaciones sobre la protección de datos personales.

15. Por otra parte, la información y los datos personales son una pieza clave e imprescindible del ciberespacio. Aunque este término tiene distintas acepciones, consideramos relevante tener presente que el ciberespacio está integrado por los siguientes elementos:

- Una infraestructura tecnológica (recursos tecnológicos) conformada por un sinnúmero de equipos (servidores, computadoras, teléfonos móviles, tabletas, etc.) que se encuentran ubicados en muchas partes del mundo;
- Una plataforma de comunicaciones (red global de comunicaciones), información y redes interconectadas (Internet) de alcance mundial denominada “infraestructura global de información”;
- Millones de personas y organizaciones de diversas nacionalidades, domiciliadas en países con sistemas jurídicos disímiles que desde cualquier parte del mundo hacen uso de la tecnología, las comunicaciones y la información para interactuar con otras personas o utilizar los servicios disponibles en Internet;
- Enormes cantidades de información (incluidos los datos personales) que circulan permanentemente dentro de los países y a través de fronteras.

16. Poco a poco vamos siendo testigos de la migración de un mundo físico contenido entre fronteras geográficas a un “ciberespacio” tecnológico sin fronteras, en el que progresivamente aumenta el número de personas que interactúan en cada momento.

17. La naturaleza global, internacional y transfronteriza de muchas actividades, como el comercio electrónico, que se lleva a cabo a través de Internet ha sido un elemento determinante que ha hecho necesario contar con una regulación apropiada para, por una parte, promover el desarrollo y la innovación y, por otra, proteger adecuadamente los derechos de las personas cuya información recolectan y utilizan empresas, personas y gobiernos en todas partes del mundo. Cabe recordar que en la Declaración sobre la Utilización del Progreso Científico y Tecnológico en Interés de la Paz y en Beneficio de la Humanidad”[12] la Asamblea General no solo reconoce que “el progreso científico y tecnológico reviste gran importancia para acelerar el desarrollo social y económico de los países en desarrollo” sino que ese progreso “al tiempo que crea posibilidades cada vez mayores de mejorar las condiciones de vida

[11] Red Iberoamericana de Protección de Datos, “Directrices para la armonización de la protección de datos en la comunidad iberoamericana”, pág. 1 (2007). A continuación, el texto señala que de este modo, el establecimiento de un marco homogéneo de regulación del derecho a la protección de datos, bien mediante la adopción de instrumentos supranacionales de carácter vinculante, bien mediante la adopción de leyes nacionales que consagren el contenido esencial de este derecho, garantizará el desarrollo del comercio en la zona, facilitando el intercambio de información entre los distintos operadores ubicados en los Estados iberoamericanos y de estos con terceros países, en particular los Estados miembros de la Unión Europea, en condiciones que no se vean restringidas como consecuencia del distinto nivel de protección del derecho fundamental a la protección de datos de carácter personal.

[12] Resolución 3384 (XXX) de la Asamblea General, de 10 de noviembre de 1975.

de los pueblos y las naciones, puede en ciertos casos dar lugar a problemas sociales, así como amenazar los derechos humanos y las libertades fundamentales del individuo". Por eso, continúa la Asamblea General, existe la "necesidad de utilizar al máximo el progreso científico y tecnológico en beneficio del hombre y de neutralizar las actuales consecuencias negativas de algunos logros científicos y tecnológicos, así como las que puedan tener en el futuro". Como consecuencia de ello, la Asamblea General acordó, entre otras cosas, que "todos los Estados adoptarán medidas eficaces, incluso de orden legislativo, para impedir y evitar que los logros científicos se utilicen en detrimento de los derechos humanos y las libertades fundamentales y la dignidad de la persona humana"[13].

II. Informes de la Relatoría Especial sobre el derecho a la privacidad respecto de temas pertinentes para actualizar la resolución 45/95

18. En un informe de 2022[14] se realizó un estudio comparativo de siete documentos internacionales para conocer el alcance de los siguientes principios sobre el tratamiento de datos personales: legalidad, licitud y legitimidad; consentimiento; transparencia; finalidad; lealtad; proporcionalidad; minimización; calidad; responsabilidad y seguridad. En él se destacaron además los elementos comunes que compartían esos documentos internacionales respecto de esos principios para crear puentes entre esos documentos o encontrar puntos de contacto que facilitaran su armonización en el contexto global.

19. En el informe se concluyó lo siguiente:

- Los principios rectores de la privacidad y de la protección de datos personales constituyen parte estructural de los sistemas jurídicos sobre la materia. Son pautas de interpretación y ayudas para completar vacíos en la legislación. Comprometen a los responsables y a los encargados a actuar de manera adecuada en el tratamiento de los datos personales.
- La legalidad debe ser el cauce por el que deben discurrir todas las actividades del tratamiento durante todo el ciclo de vida de los datos personales y tiene como requisito base la configuración de algunas de las causales legitimantes establecidas en la normativa que sea de aplicación.
- El principio de consentimiento está íntimamente unido al de legalidad, siendo la causa habilitante para el tratamiento de los datos personales más común, internacionalmente reconocida.
- El principio de transparencia debe observarse independientemente de cuál sea la base jurídica que legitima el tratamiento.
- El principio de finalidad se encuentra establecido en todos los documentos normativos analizados. La finalidad debe ser: explícita, específica, legítima y pertinente. Funcionará como delimitadora de las actividades de tratamiento a las que serán sometidos los datos personales.
- La lealtad exige que la información personal sea tratada respetando de manera fiel todos los términos y condiciones que habilitaron su recopilación y utilizando medios para el tratamiento que faciliten dicho objetivo.

[13] *Ibid.*, párr. 8.

[14] "Principios que informan la privacidad y la protección de datos personales", Informe de la Relatora Especial sobre el derecho a la privacidad (A/77/196, 20 de julio de 2022).

- Por el principio de proporcionalidad los datos personales, así como las actividades de tratamiento a los que aquellos sean sometidos, deben limitarse únicamente al cumplimiento de los fines legítimos para los cuales fueron recopilados.
- La calidad de la información personal que esté siendo objeto de tratamiento, resulta vital para el buen logro de las finalidades que autorizaron su recopilación, así como su posterior tratamiento.
- El principio de responsabilidad tiende a reforzar y hacer que el deber del cumplimiento de los principios y de la normativa pase a contar con elementos objetivos en los que el cumplimiento real se sustente y se logren los fines legítimos, en un clima de confianza y respeto de los derechos fundamentales involucrados.
- No habrá protección de datos ni respeto a la privacidad sin seguridad. Garantizar la integridad, disponibilidad y confidencialidad de los datos personales es una tarea primordial y una gran responsabilidad. La diversidad de las tecnologías, así como su dinámica transformación, deben ser tomadas en cuenta para evaluar con responsabilidad y ética, los riesgos y las medidas de seguridad adecuadas.
- Existen muchos puntos comunes, a la hora en que los documentos normativos internacionales desarrollan los principios de la privacidad y de la protección de datos personales.
- Los elementos comunes identificados, pueden servir de base para avanzar hacia un consenso global que permitirá hacer frente, de manera conjunta y adecuada, a los distintos retos que se presentan en el tratamiento de los datos que conciernen a las personas, tales como los relacionados con la transferencia internacional de datos, el uso de las tecnologías de la información y de las comunicaciones, la inteligencia artificial, en tanto los derechos humanos merecen igual respeto en entornos virtuales como presenciales.
- Es menester continuar avanzando hacia un equilibrio entre los distintos intereses involucrados en el tratamiento de datos personales en la era global y digital en la que nos encontramos, en pos de la cooperación y la armonización normativa[15].

20. En un informe 2021 sobre la inteligencia artificial y la privacidad, así como la privacidad de los niños[16], se señaló lo siguiente:

21. En primer lugar, en relación con la privacidad de los niños, se concluyó que era necesario, entre otras cosas, aprobar políticas, legislación y normas que:

- Consideren a los niños como titulares de derechos humanos, con un derecho inalienable a la intimidad, la autonomía y la igualdad;
- Incorporen el alcance general de la privacidad, y no solo en relación con la protección de datos, para permitir el pleno desarrollo del potencial de los niños;
- Incorporen en las políticas públicas las opiniones de los niños, las estrategias de estos respecto de la privacidad, las conclusiones de investigaciones centradas en los niños y/o las evaluaciones del impacto en la privacidad de los niños;

[15] *Ibid.*, párrs. 138 a 150.

[16] "La inteligencia artificial y la privacidad, así como la privacidad de los niños", Informe del Relator Especial sobre el derecho a la privacidad (A/HRC/46/37, 25 de enero de 2021).

- Proporcionen medios independientes para conciliar, arbitrar y reparar en el caso de vulneraciones individuales o sistémicas de los derechos humanos de los niños; y aseguren la adopción de medidas coercitivas en caso de infracción[17].

22. Además, se recomendó lo siguiente:

- Velar por que no se recopilen datos biométricos de los niños, salvo como medida excepcional, y únicamente cuando sea legal, necesario, proporcionado, y respetando plenamente los derechos del niño;
- Velar por que los datos personales de los niños se traten de forma justa, precisa y segura, con una finalidad específica y de acuerdo con una base jurídica legítima, utilizando marcos de protección de datos que representen las mejores prácticas, como el Reglamento General de Protección de Datos y el Convenio 108+;
- Velar por que quienes tratan los datos personales, incluidos los padres o cuidadores y los educadores, sean conscientes del derecho de los niños a la privacidad y a la protección de los datos;
- Velar por que los niños tengan acceso a información sobre el ejercicio de sus derechos, por ejemplo, en los sitios web de las autoridades encargadas de la protección de datos, y que haya a su disposición asesoramiento, mecanismos de reclamación y medidas de reparación que sean específicos para los niños, también en caso de ciberacoso;
- Prohibir el tratamiento automatizado de los datos personales que elaboran perfiles de niños para la toma de decisiones que les conciernen o para analizar o predecir las preferencias personales, el comportamiento y las actitudes, salvo en circunstancias excepcionales en razón del interés superior del niño o de un interés público superior y con las garantías legales adecuadas[18].

23. En segundo lugar, se presentaron recomendaciones sobre la protección de la privacidad en el desarrollo y la aplicación de soluciones de inteligencia artificial, con el propósito de "proporcionar directrices sobre el uso de la información personal y no personal en el contexto de las soluciones de inteligencia artificial (IA) desarrolladas como parte de las tecnologías de la información y las comunicaciones (TIC) aplicadas, así como hacer hincapié en la importancia de una base legítima para el tratamiento de datos de IA por parte de los Gobiernos y las empresas en el marco general del derecho humano a la privacidad"[19].

24. En el informe se puso de relieve que tanto el tratamiento de los datos como la decisión que se adoptara como resultado de ese tratamiento mediante herramientas de inteligencia artificial (IA) entrañaban riesgos potenciales para los titulares de los datos. Por eso, se consideró importante señalar unos principios que habían de tenerse en cuenta a la hora de planificar, desarrollar y aplicar soluciones de IA, a saber: a) jurisdicción; b) base ética y legal; c) fundamentos de los datos; d) responsabilidad y supervisión; e) control; f) transparencia y "justificación"; g) derechos del titular de los datos; y h) salvaguardias.

[17] *Ibid.*, párr. 126.
[18] *Ibid.*, párr. 127.
[19] *Ibid.*, párr. 1.

25. En un informe posterior, se hizo referencia a los principios de transparencia y explicabilidad en el tratamiento de datos personales en la inteligencia artificial y se recalcó la importancia de esos principios en ese contexto[20].

26. Esos principios son relevantes porque la transparencia y la explicabilidad no solo ayudan a generar confianza y fiabilidad en la inteligencia artificial, sino que contribuyen a proteger los derechos humanos. Mediante esos principios, por una parte, se informa de manera oportuna, completa, sencilla y clara a las personas sobre aspectos básicos respecto del uso de su información personal en procesos o proyectos de inteligencia artificial y sus consecuencias y, por otra parte, se exige que las personas afectadas por la inteligencia artificial puedan conocer los motivos concretos por los cuales se han visto afectadas. De este modo, esas personas podrán ejercer sus derechos, por ejemplo, el derecho al debido proceso y el derecho de defensa frente a las decisiones que se hayan adoptado mediante la utilización de herramientas o tecnologías de inteligencia artificial.

27. En ese informe se recalcó que la inteligencia artificial conllevaba diferentes tipos de riesgos. Entre las contingencias que había de tenerse en cuenta debían considerarse las inherentes a la operación de los algoritmos —sesgos humanos, fallas técnicas, vulnerabilidad de seguridad y fallas en la implementación—, a su diseño y al tratamiento de datos personales.

28. En cuanto a los datos personales, se señaló que estos eran un insumo que procesaban los algoritmos para arrojar resultados. Los datos de entrada podían estar afectados por sesgos (incorporación de datos parciales, insuficientes, no actualizados o manipulados) o su pertinencia (relevancia, inconsistencia o completitud de los datos). Si no se usan datos de calidad que sean pertinentes, los resultados serán erróneos. El algoritmo, por su parte, puede verse afectado por los patrones (sesgos de la lógica de programación, inclusión de funciones no previstas y fallas inherentes de las funciones utilizadas para su codificación) y los errores (condiciones de la operación que reflejan un funcionamiento diferente al previsto y que atentan contra las premisas del diseño planteado). Todo lo anterior incide en los resultados obtenidos con herramientas de IA, que están relacionados con la pertinencia y precisión del resultado de la ejecución del algoritmo y constituyen una respuesta al análisis de los datos de entrada.

29. Estas son algunas de las conclusiones de ese informe:

a) La transparencia y la explicabilidad contribuyen a generar confianza en la inteligencia artificial y a respetar los derechos humanos;

b) Quienes desarrollan inteligencia artificial deben ser transparentes con relación a cómo se tratan los datos (cómo se recopilan, almacenan y utilizan), así como también con relación a la forma en que se toman las decisiones basadas en la inteligencia artificial, la confiabilidad de estas y la seguridad de la información;

c) Las personas afectadas por las decisiones tomadas a partir de la inteligencia artificial merecen una explicación clara, sencilla, completa, veraz y comprensible de la motivación de esa decisión. En este sentido, el principio de explicabilidad es de cardinal importancia no solo porque se corresponde con el principio de transparencia, sino porque permitirá el derecho de defensa y el debido proceso de dichas personas;

d) La explicabilidad y la transparencia demandan claridad, completitud, veracidad, imparcialidad y publicidad de las decisiones adoptadas mediante

[20] “Principios de transparencia y explicabilidad en el tratamiento de datos personales en la inteligencia artificial”, Informe de la Relatora Especial sobre el derecho a la privacidad (A/78/310, 30 de agosto de 2023).

inteligencia artificial y de la lógica, método o razonamiento para tomar decisiones sobre los seres humanos a partir de la información y, particularmente, los datos personales. La explicabilidad y la transparencia se oponen, desde luego, a la opacidad, la oscuridad, el engaño, la mentira y el abuso del poder informático, los cuales son algunos síntomas de un tratamiento de datos ilegal carente de ética y respeto por los seres humanos y su dignidad [21].

30. Además, se formularon las siguientes recomendaciones:

a) Promover la transparencia en la inteligencia artificial para mitigar los riesgos que la opacidad pueda generar en la sociedad y, especialmente, respecto de la protección de los derechos humanos;

b) Incorporar en las regulaciones el principio de explicabilidad, no solo para que las personas comprendan cómo se adoptaron las decisiones que las afectan, sino para que puedan tener herramientas para defender sus derechos humanos frente a la inteligencia artificial;

c) Fomentar prácticas éticas que aseguren la transparencia y la explicabilidad en el tratamiento de datos personales en los proyectos o procesos de inteligencia artificial;

d) Impulsar, apoyar y facilitar la educación y la alfabetización digital para que los ciudadanos comprendan mejor los conceptos relacionados con la inteligencia artificial, la transparencia y la explicabilidad, de manera que puedan exigir el respeto de sus derechos [22].

31. Por otra parte, en un informe de 2024 [23] se realizó un estudio comparativo sobre los mecanismos legales de salvaguarda para la protección de datos personales y la privacidad en la era digital. También se examinaron los mecanismos legales de los que disponían los titulares de los datos personales para la atención de sus derechos, su restitución y, en su caso, la reparación del daño generado por el uso indebido de la información que les concerniese.

32. Estas son algunas de las conclusiones de ese informe:

a) En países de los cinco continentes se da el reconocimiento expreso en sus legislaciones de diversos derechos que corresponden a los titulares de los datos personales y que les permiten el control sobre su información personal;

b) Algunas legislaciones van avanzando al reconocer nuevos derechos como los vinculados al tratamiento de datos automatizado y digitalizado o en el contexto de Internet, de las redes sociales y servicios equivalentes. Asimismo, el avance puede apreciarse a través del reconocimiento expreso más detallado de determinados derechos;

c) Los derechos de los titulares de los datos personales se ejercen ante el responsable del tratamiento a través de procedimientos regulados, en cada ordenamiento jurídico, que poseen semejanzas y particularidades;

d) Entre los aspectos regulados del procedimiento para el ejercicio de los derechos ante el responsable del tratamiento se encuentran, de manera específica según determinadas leyes, la facultad del titular o su representante para presentar la solicitud de ejercicio de un derecho, las formas de las posibles respuestas, los medios

[21] *Ibid.*, párr. 63.
[22] *Ibid.*, párr. 64.
[23] "Mecanismos legales de salvaguarda para la protección de datos personales y la privacidad en la era digital", Informe de la Relatora Especial sobre el derecho a la privacidad (A/HRC/55/46, 18 de enero de 2024).

de respuesta; el plazo para responder; la gratuidad u onerosidad, y el deber de informar, ante la denegatoria de la solicitud del derecho, de la posibilidad que tiene el titular para presentar una reclamación ante una autoridad administrativa o jurisdiccional;

e) En la tutela administrativa, a la que puede recurrir el titular no atendido en su derecho o después de denegado este, por parte del responsable del tratamiento, existen aspectos de regulación convergente. Entre las particularidades contenidas en determinadas legislaciones se encuentran la gratuidad de la reclamación, el plazo para resolver y la posibilidad de derivación a un esquema alternativo de resolución de conflictos;

f) Como parte de la tutela administrativa, en las distintas leyes se consideran medidas destinadas a la atención del derecho solicitado, y algunas tienen como objetivo evitar que se siga cometiendo la infracción y que la conducta se produzca nuevamente;

g) En algunas legislaciones se considera expresamente la apelación de las resoluciones de la autoridad de control ante un órgano administrativo superior, así como la impugnación de las resoluciones de la autoridad de control ante determinados órganos jurisdiccionales como parte del derecho a la tutela judicial efectiva;

h) Con el fin de obtener la tutela del derecho a la protección de datos personales, que ha sido denegado o no atendido por el responsable del tratamiento, algunas leyes brindan al titular la posibilidad de elegir si recurre ante la autoridad administrativa de control o si debe dirigirse directamente al poder judicial, ante el órgano competente;

i) Los cinco países analizados regulan en mayor o menor medida determinados aspectos de la vía reparatoria, que es a la que puede recurrir el titular de los datos personales que haya sufrido daños y perjuicios como consecuencia de una infracción en la legislación sobre protección de datos y privacidad[24].

33. Entre las principales recomendaciones de ese informe, se exhortó a los Estados a que:

a) Establezcan multidisciplinariamente marcos jurídicos actualizados y apropiados, con el apoyo de todos los actores involucrados y, en particular, que aprueben leyes y reglamentos adecuados que instauren mecanismos de tutela accesibles y oportunos para la atención, reparación y restitución efectivas del derecho a la protección de datos personales, así como para el resarcimiento del daño causado por la violación de la normativa sobre la materia;

b) Dentro de su soberanía, identifiquen y evalúen la adopción de aspectos regulatorios de otras legislaciones sobre protección de datos y privacidad que permitan brindar mayores garantías para el respeto efectivo de estos derechos en la era digital;

c) Promuevan y favorezcan de forma prioritaria la información y educación en materia de derechos humanos, en particular sobre la protección de datos personales y la privacidad, en todos los niveles y en todos los campos, con el fin de que las personas titulares de la información conozcan, comprendan y estén en capacidad de ejercer sus derechos y, en su caso, de acudir a los mecanismos de tutela para garantizar la efectividad de estos [25].

[24] *Ibid.*, párr. 123.
[25] *Ibid.*, párr. 124.

34. Por otra parte, en 2022 se presentó un informe[26] sobre la implementación de los principios de finalidad, eliminación y responsabilidad demostrada o proactiva en el tratamiento de datos personales recolectados por entidades públicas con ocasión de la pandemia de COVID-19, con miras a verificar qué había pasado, qué estaba pasando o qué pasaría con los datos de millones de personas de todos los países del mundo que se habían recolectado para combatir la pandemia.

35. A partir del análisis de 20 países de África, América, Asia, Europa y Oceanía se emitieron algunas conclusiones y se formularon las siguientes recomendaciones:

- Verificar el cumplimiento real y efectivo de los principios de finalidad, eliminación y responsabilidad demostrada o proactiva respecto de los datos de millones de personas que fueron recolectados con el propósito de detectar y/o combatir la COVID-19, así como rastrear su propagación para proteger la salud y prevenir su trasmisión.
- Reforzar la aplicación del principio de responsabilidad demostrada o proactiva en todos los proyectos o políticas que impliquen el tratamiento de datos personales. Esto requiere, entre otros aspectos, adoptar medidas útiles, apropiadas, oportunas y efectivas para cumplir las obligaciones legales establecidas en la regulación sobre el tratamiento de datos personales. Dichas medidas deben ser objeto de revisión y evaluación permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales.
- Implementar procesos y utilizar herramientas que evidencien y demuestren el correcto cumplimiento de sus deberes. Estos procesos y herramientas deben ser transparentes y de fácil verificación por parte de las autoridades públicas competentes y de la ciudadanía.
- Antes de iniciar el diseño y la elaboración de aplicaciones y programas informáticos que involucren el tratamiento de datos personales para cumplir funciones del Estado, se sugiere a los Estados que implementen medidas proactivas y preventivas con el fin de poner en funcionamiento un sistema de vigilancia y de manejo de riesgos para garantizar que los datos se tratarán debidamente y de conformidad con la regulación existente.
- Fortalecer una cultura pública que fomente un tratamiento de datos personales con todas las garantías, transparente y ético, de manera que este tipo de tratamiento sea un componente esencial del diseño y puesta en marcha de proyectos o políticas públicas que requieran el tratamiento de datos personales.
- Incrementar y consolidar los niveles de confianza ciudadana respecto de los proyectos de entidades públicas que involucran el tratamiento de datos personales mediante la implementación de mecanismos transparentes y de acceso público que permitan a la ciudadanía constatar, en todo momento y de manera sencilla, que las entidades públicas cumplen en la práctica lo que anuncian o prometen en sus políticas o términos y condiciones de actividades que implican la recolección, el uso, la circulación o cualquier otra actividad en la que se traten datos personales [27].

[26] "Implementación de los principios de finalidad, eliminación y responsabilidad demostrada o proactiva en el tratamiento de datos personales recolectados por entidades públicas con ocasión de la pandemia de COVID-19", Informe de la Relatora Especial sobre el derecho a la privacidad (A/HRC/52/37, 27 de diciembre de 2022).

[27] *Ibid.*, párrs. 27 a 32.

III. Algunas lagunas temáticas de la resolución 45/95 en comparación con documentos internacionales sobre el tratamiento de datos personales

36. Dado se aprobó en 1990, la resolución 45/95, ha quedado rezagada en cuanto a su contenido respecto de documentos internacionales posteriores. Esto puede constatarse haciendo un análisis comparativo de la resolución con los siguientes documentos:

- Marco de Privacidad del APEC, de 2004.
- "Estándares internacionales sobre protección de datos personales y privacidad: propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal" (Resolución de Madrid, 2009).
- Recomendación del Consejo de la OCDE relativa a las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, no disponibles en español), de 2013.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (27 de abril de 2016) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Estándares de Protección de Datos Personales para los Estados iberoamericanos de la Red Iberoamericana de Protección de Datos[28], aprobados en 2017.
- Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108+), del Consejo de Europa, 2018.
- Principios actualizados sobre la privacidad y la protección de datos personales, de la Organización de los Estados Americanos, de 2021[29].
- Resolución sobre los estándares globales de protección de datos, en la que figuran principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo", de la GPA (2023)[30].

37. Los principales resultados del análisis comparativo son los siguientes:

Primero: en cuanto a los principios sobre tratamiento de datos personales, la resolución 45/95 no contiene los siguientes: legitimación, transparencia, responsabilidad demostrada y confidencialidad, como surge del siguiente cuadro:

[28] Documento aprobado en el XV Encuentro Iberoamericano de Protección de Datos de la Red Iberoamericana de Protección de Datos, que tuvo lugar en Santiago de Chile, el 22 de junio de 2017.

[29] Los Principios fueron adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la Organización de los Estados Americanos en 2021.

[30] Véase la nota 9.

Cuadro 1
Principios sobre el tratamiento de datos personales que se mencionan expresamente en documentos internacionales

Principio	*Naciones Unidas (1990)*	*APEC (2004)*	*CIAPDP (2009)*	*OCDE (2013)*	*UE (2016)*	*RIPD (2017)*	*C 108+ (2018)*	*OEA (2021)*	*GPA (2023)*
Legitimación	■								
Licitud									
Lealtad /buena fe		■							
Transparencia	■								
Finalidad									
Proporcionalidad									
Calidad									
Responsabilidad	■								
Seguridad									
Confidencialidad	■	■		■					
Temporalidad		■	■	■					
Prevención del daño			■	■	■	■	■		
No discriminación		■	■	■	■	■	■		

Significado: **No** ■ **Si**

Segundo: en cuanto a los derechos de los titulares de los datos personales, la resolución 45/95 no contiene los siguientes: oposición, portabilidad, no ser objeto de decisiones individuales automatizadas e indemnización de perjuicios, como se muestra en el siguiente cuadro:

Cuadro 2
Derechos de la persona titular de los datos que se mencionan expresamente en documentos internacionales

Derechos	*Naciones Unidas (1990)*	*APEC (2004)*	*CIAPDP (2009)*	*OCDE (2013)*	*UE (2016)*	*RIPD (2017)*	*C 108+ (2018)*	*OEA (2021)*	*GPA (2023)*
Acceso									
Rectificación									
Cancelación / supresión		■		■					
Oposición	■	■		■					
Portabilidad	■	■	■	■			■		
No ser objeto de decisiones individuales automatizadas	■	■		■				■	
Indemnización de perjuicios	■	■	■	■			■		

Significado: **No** ■ **Si**

Tercero: en cuanto a las medidas proactivas en el tratamiento de datos, la resolución mencionada no incorpora las que siguen a continuación: privacidad por diseño, privacidad por defecto, oficial o delegado de protección de datos, mecanismos de autorregulación y evaluación de impacto relativa a las protección de datos, como se muestra en el siguiente cuadro:

Cuadro 3
Medidas proactivas para el tratamiento de datos personales que se mencionan expresamente en documentos internacionales

Medida proactiva	*Naciones Unidas (1990)*	*APEC (2004)*	*CIAPDP (2009)*	*OCDE (2013)*	*UE (2016)*	*RIPD (2017)*	*C 108+ (2018)*	*OEA (2021)*	*GPA (2023)*
Privacidad por diseño	■		■	■					
Privacidad por defecto	■	■	■	■			■		
Oficial o Delegado de protección de datos	■	■	■	■				■	
Mecanismos de autorregulación	■						■		
Evaluación de impacto relativa a la protección de datos	■			■					

Significado: **No** ■ **Si**

Cuarto: en cuanto a las alternativas para realizar transferencias internacionales de datos, la resolución omite las siguientes: uso de cláusulas contractuales, normas corporativas vinculantes, mecanismos de certificación, autorización de la autoridad de control, autorización del titular de los datos y tratados internacionales, como se muestra en el siguiente cuadro:

Cuadro 4
Alternativas para realizar transferencias internacionales de datos personales que se mencionan expresamente en documentos internacionales

Alternativas	*Naciones Unidas (1990)*	*APEC (2004)*	*CIAPDP (2009)*	*OCDE (2013)*	*UE (2016)*	*RIPD (2017)*	*C 108+ (2018)*	*OEA (2021)*	*GPA (2023)*
Nivel adecuado de protección/ garantías comparables				■					
Cláusulas contractuales	■	■		■					
Normas corporativas vinculantes	■	■						■	■
Mecanismos de certificación	■	■	■	■			■	■	
Autorización de la autoridad de control	■		■	■				■	■
Autorización del titular del dato	■	■	■	■				■	■
Tratados internacionales	■	■	■	■				■	■

Significado: **No** ■ **Si**

Quinto: en cuanto a los requisitos o características que deben cumplir las autoridades de control o de protección de datos personales, la resolución no menciona los siguientes: gozar las autoridades de autonomía; ser ajenas a toda influencia externa; contar con poderes de investigación, supervisión, sanción y promoción; y tener suficientes recursos humanos y materiales para cumplir sus funciones, como se muestra en el siguiente cuadro:

Cuadro 5
Requisitos que exigen expresamente documentos internacionales sobre las autoridades de control o protección de datos personales

Requisitos	*Naciones Unidas (1990)*	*APEC (2004)*	*CIAPDP (2009)*	*OCDE (2013)*	*UE (2016)*	*RIPD (2017)*	*C 108+ (2018)*	*OEA (2021)*	*GPA (2023)*
Autonomía	■	■	■	■				■	
Imparcialidad		■		■				■	■
Independencia		■							
Ajena a toda influencia externa	■	■	■				■	■	■
Poderes de investigación, supervisión, sanción y promoción	■	■							
Recursos humanos y materiales suficientes	■	■	■	■					
Competencia técnica		■					■	■	

Significado: ■ **No** **Si**

Dados los resultados del análisis indicados, la propuesta de actualización incorpora los temas no previstos actualmente en la resolución 45/95 para que esta sea completa y suficiente, con miras a dar respuesta a las necesidades actuales para garantizar el debido tratamiento de los datos personales.

Por lo tanto, se propone a la Asamblea General que apruebe el siguiente texto de modificación de la resolución 45/95, de 14 de diciembre de 1990:

Texto de la propuesta de modificación de la resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990

Principios rectores para el tratamiento de datos personales

Las modalidades de aplicación de los reglamentos relativos al tratamiento de datos personales se dejan a la libre iniciativa de cada Estado con sujeción a las siguientes orientaciones:

A. Principios relativos a las garantías mínimas que deberían preverse en la legislación nacional para el debido tratamiento de los datos personales

1. Principio de licitud y lealtad

La recolección, uso, circulación, tratamiento o cualquier actividad con datos personales debe realizarse conforme a la legislación de cada país y para fines lícitos.

Las informaciones relativas a las personas (datos personales) no se deberán recoger ni tratar mediante procedimientos desleales, engañosos, ilícitos o fraudulentos ni utilizarse con fines contrarios a la dignidad humana o los propósitos y principios de la Carta de las Naciones Unidas.

2. Principio de exactitud o calidad de los datos

Los datos personales deberán ser veraces, completos, exactos, actualizados, comprobables, pertinentes respecto de la finalidad del tratamiento y deberán actualizarse siempre que sea necesario, ya sea de oficio, por parte del responsable, encargado, o a petición del interesado. No debe permitirse el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Los responsables o encargados del tratamiento de datos personales deberán adoptar medidas para garantizar la calidad, la actualización, la completitud, la exactitud y la pertinencia de la información.

3. Principio de finalidad, necesidad, proporcionalidad y temporalidad

El tratamiento de los datos debe limitarse al cumplimiento de fines específicos, explícitos y legítimos y no tratarse posteriormente de manera incompatible con dichas finalidades. Solo deben tratarse los datos que sean necesarios, pertinentes y apropiados para cumplir los objetivos del tratamiento. Los datos deben ser limitados y no deben ser excesivos con relación a la finalidad para la cual fueron recolectados.

La finalidad del tratamiento de datos personales deberá especificarse y justificarse y, en el momento de recolección de dicha información, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada (titular de los datos) a fin de que ulteriormente sea posible asegurarse de que: a) todos los datos personales reunidos, registrados u objeto de tratamiento siguen siendo pertinentes a la finalidad perseguida; b) ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, o con un propósito incompatible con el que se haya especificado; c) el período de conservación de los datos personales no excede del necesario para alcanzar la finalidad autorizada o permitida para el tratamiento de los datos personales.

Los datos personales deben conservarse únicamente durante el tiempo que sea necesario para cumplir con los fines para los que se recolectan o tratan, y deben eliminarse o anonimizarse cuando ya no sean necesarios para esos fines.

4. Principio de acceso de la persona interesada (titular de los datos)

Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada o a conocer los destinatarios. Debería preverse una vía de recurso, en su caso, ante la autoridad encargada de controlar el respeto de los principios. En caso de rectificación, el costo debería sufragarlo el responsable o encargado del tratamiento de los datos personales. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

5. Principio de no discriminación y manipulación

A reserva de las excepciones previstas con criterio limitativo en el principio 6, no deben registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico de una persona, sus convicciones religiosas, filosóficas o de otro tipo, o sobre su participación en una asociación o afiliación a un sindicato u organizaciones sociales o de derechos humanos o que promueva intereses de cualquier partido político o que garantice los derechos de partidos políticos de oposición, así

como los datos relativos a la salud, la vida sexual o preferencias sexuales y los datos genéticos y biométricos dirigidos a identificar de manera unívoca a una persona física o los datos neuronales.

El tratamiento de datos neuronales o neurodatos no podrá utilizarse para manipular o alterar la libertad de pensamiento y conciencia de una persona, haciendo que esta sea dependiente de un tercero, afectando sus ideas, seguridad e independencia, así como su identidad cerebral natural e integridad neurocognitiva. Tampoco se podrá tratar esos datos para finalidades diferentes a la promoción de la salud, el diagnóstico, la rehabilitación y la paliación de enfermedades en el contexto del derecho a la salud, o la investigación científica en el campo de la biología, la psicología y la medicina, orientados a aliviar el sufrimiento o mejorar la salud.

6. Facultad de establecer excepciones

Solo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente en la ley o en una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas.

Las excepciones al principio 5, relativo a la prohibición de discriminación, deberían estar sujetas a las mismas garantías que las previstas para las excepciones a los principios 1 a 4 y solo podrían autorizarse dentro de los límites previstos por la Declaración Universal de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

7. Principio de seguridad

Se deberán adoptar medidas preventivas, apropiadas, razonables, suficientes, útiles y oportunas para proteger los ficheros, bases de datos o sistemas de información contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos, la contaminación por virus informático, la manipulación, pérdida, modificación, destrucción, daño o divulgación de la información u otro uso indebido.

Las medidas de seguridad deberán ser objeto de auditoría, revisión, mantenimiento y actualización permanente aplicables al tratamiento de los datos personales, de manera periódica.

También deberán adoptarse medidas para gestionar adecuada y oportunamente eventuales incidentes de seguridad con el objetivo de evitar que se causen daños a los titulares de los datos, los responsables, los encargados y la sociedad en general.

8. Principio de confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, incluso después de finalizada su relación con alguna de las actividades que comprende el tratamiento, pudiendo solo suministrar o comunicar datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la ley o por el titular de los datos.

9. Protección reforzada de datos sensibles

Existen datos sensibles que afectan la intimidad del titular de los datos o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos o a organizaciones sociales o de derechos humanos o que promuevan intereses de cualquier partido político o que aseguren los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, la vida sexual o preferencias sexuales, los neurodatos (datos neuronales) y los datos genéticos y biométricos dirigidos a identificar de manera unívoca a una persona física.

Esta información sensible deberá ser objeto de medidas especiales de responsabilidad reforzada de manera que existan mayores medidas de seguridad, confidencialidad, acceso y circulación restringida para evitar el acceso a esa información o su uso indebido, así como su manipulación o destrucción.

10. Protección especial de datos personales de niñas, niños y adolescentes

En el tratamiento de datos personales concernientes a niñas, niños y adolescentes se privilegiará la protección del interés superior de estos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

Se promoverá, en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías y se alertará de los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, y se fomentará el respeto de sus libertades y derechos, y los derechos de los demás.

Los datos personales de las niñas, los niños y adolescentes deberían ser objeto de medidas especiales de responsabilidad reforzada de manera que existan mayores medidas de seguridad, confidencialidad, acceso y circulación restringida para evitar el acceso a esos datos o su uso indebido, así como su manipulación o destrucción.

11. Principio sobre las decisiones individuales automatizadas

El titular de los datos tendrá derecho a no ser objeto de decisiones que produzcan efectos jurídicos que le conciernan o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del titular o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Lo anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable, cuando ese tratamiento esté autorizado por el derecho interno de los Estados o cuando se base en el consentimiento demostrable del titular.

No obstante, cuando sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento, el titular tendrá derecho a obtener la intervención humana, recibir una explicación sobre la decisión tomada, expresar su punto de vista e impugnar la decisión.

12. Principio de transparencia

Antes de que se recopilen los datos o en ese momento, se deberán especificar la identidad y los datos de contacto del responsable de los datos, las finalidades

específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información que se transmitirá y los derechos del titular en relación con los datos personales que han de recopilarse. Cuando el tratamiento de los datos se base en el consentimiento, los datos personales solamente deberán ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran.

En el caso de que el titular de los datos sea objeto de decisiones automatizadas, en la elaboración de perfiles o en los procesos de decisión mediante inteligencia artificial u otras tecnologías, se le deberá comunicar de manera clara y sencilla lo siguiente:

- Los procesos de automatización, inteligencia artificial o cualquier otra tecnología que se utilizarán para el tratamiento de sus datos personales.
- Información clara, veraz y significativa sobre la lógica aplicada para tomar una decisión que lo afecta de manera que pueda conocer los aspectos básicos sobre la toma de decisiones a partir de sus datos personales.
- La información que se utilizará para adoptar dicha decisión.
- La existencia o no de supervisión humana cualificada para verificar la calidad de la decisión.
- Información adicional que permita al titular de los datos conocer la forma en que las decisiones automatizadas pueden afectarlo positiva o negativamente. La información se debe suministrar en un lenguaje claro, sencillo y de fácil comprensión.

13. Principio de explicabilidad

Cuando lo solicite el titular de los datos, el responsable o encargado deberá proporcionar explicaciones en un lenguaje claro y comprensible respecto de la información y el proceso realizado para adoptar una decisión que afecta a dicha persona.

Dicha explicación no solo deberá reflejar de manera precisa el razonamiento del sistema utilizado para tomar la decisión, sino que deberá ser comprensible, veraz, completa, fácilmente entendible y específica o concreta en el caso del titular afectado. Se deberá suministrar toda la información y las explicaciones necesarias para que las personas comprendan cómo se adoptaron las decisiones que las afectan y para que puedan tener herramientas para defender sus derechos humanos o solicitar la revisión de la decisión.

Además, se deberá contar con un ser humano responsable a quien no solo se le puedan plantear las preocupaciones u objeciones relacionadas con las decisiones automatizadas y se puedan ejercer los derechos, sino que pueda impulsar la evaluación y revisión del proceso automatizado de decisión.

14. Principio de responsabilidad demostrable o proactiva (*accountability*)

Los responsables y encargados del tratamiento de datos deberán adoptar e implementar medidas técnicas, organizacionales y de otra naturaleza que sean útiles, oportunas, apropiadas y efectivas para garantizar y demostrar que el tratamiento se realiza de conformidad con los principios expuestos en la presente resolución.

Dichas medidas deberán ser auditadas y actualizadas de forma periódica para establecer que están funcionando correctamente y medir el grado de protección

de los derechos de los titulares de los datos y de cumplimiento de estos principios.

15. Evaluaciones del impacto del tratamiento de datos

Cuando sea probable que un tipo de tratamiento, en particular si se utilizan nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes de llevarlo a cabo, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales con miras a adoptar medidas preventivas para afrontar y mitigar los riesgos identificados.

La evaluación del impacto se deberá realizar, entre otras cosas, cuando se vayan a evaluar de manera sistemática y exhaustiva aspectos personales de personas físicas que se basen en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; o cuando se pretenda realizar un tratamiento masivo o a gran escala de datos sensibles o de datos de menores de edad.

16. Privacidad desde el diseño y por defecto

Teniendo en cuenta de forma razonable los costos de aplicación del tratamiento, el estado de la técnica, la naturaleza, circunstancias y fines del tratamiento, así como el riesgo probable que conlleve y su gravedad, el responsable del tratamiento de datos (y eventualmente el encargado) deberán aplicar medidas técnicas y organizativas apropiadas para que, al momento de determinar los medios de tratamiento aplicables y durante el tratamiento mismo se hagan efectivos los principios de la presente resolución.

Además, también deberán aplicar dichas medidas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplica también a la cantidad de datos que han de tratarse, la extensión del tratamiento, el plazo de conservación de los datos y su accesibilidad.

17. Principio de precaución

En caso de que no hubiera certeza acerca de los daños que podrían causarse al titular de los datos o a la sociedad con ocasión del tratamiento de los datos personales, y con miras a evitar que se produzca un daño grave e irreversible, el responsable o encargado del tratamiento deberá abstenerse de realizar dicho tratamiento o de adoptar medidas precautorias o preventivas para proteger los derechos del titular de los datos, su dignidad humana y otros derechos humanos.

El principio de precaución también se aplica cuando el riesgo que se corra o la magnitud del daño producido o que pueda sobrevenir no son conocidos con anticipación, porque no hay manera de establecer, a mediano o largo plazo, los efectos que tendría el tratamiento de los datos.

18. Principio de favorabilidad o preeminencia

En caso de duda sobre la interpretación y la aplicación de estos principios, prevalecerá la que sea más favorable al titular de los datos personales.

19. Principio de autorregulación

El responsable del tratamiento podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otras cosas, contribuir a la correcta aplicación de estos principios y establecer

procedimientos de resolución de conflictos entre el responsable y el titular de los datos, sin perjuicio de otros mecanismos que establezca la legislación nacional de la materia aplicable, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular.

A los efectos del párrafo anterior, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en este artículo.

20. Principio de efectiva protección de los derechos de los titulares de los datos personales

Se adoptarán mecanismos útiles, efectivos, simples y expeditos para garantizar los siguientes derechos de las personas que sean titulares de los datos personales: acceso, rectificación, cancelación (supresión), oposición, portabilidad, no ser objeto de decisiones automatizadas que produzcan efectos jurídicos que les conciernan o les afecten de manera significativa e indemnización de perjuicios ocasionados al titular de los datos por el indebido tratamiento de su información.

Además de las acciones judiciales o administrativas previstas en la regulación nacional, se promoverán el uso de alternativas de solución de controversias sobre el tratamiento de datos personales.

21. Control y sanciones

Cada Estado deberá designar a la autoridad que, de conformidad con el sistema jurídico interno, se encargue de controlar el respeto de los principios expuestos en la presente resolución. Dicha autoridad deberá ofrecer garantías de imparcialidad, de independencia con respecto a las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de competencia técnica. En caso de violación de las disposiciones de la legislación interna promulgada en virtud de los principios anteriormente enunciados, deberán preverse sanciones penales y de otro tipo, así como recursos individuales apropiados.

La autoridad deberá contar con plena autonomía y será ajena a toda influencia externa, directa o indirecta, y no solicitará ni admitirá orden ni instrucción alguna. Su equipo deberá contar con experiencia y conocimientos especializados sobre el tratamiento de datos personales.

La autoridad será designada mediante un procedimiento público y transparente por un período de tiempo determinado. Las personas designadas no podrán ser removidas sino por causales graves previamente establecidas en la regulación de cada país.

La autoridad deberá contar con suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que sean necesarios para garantizar los derechos de los titulares de los datos y el debido tratamiento de su información. También deberán tener suficientes recursos económicos, humanos y tecnológicos para cumplir debida y oportunamente sus funciones.

22. Flujo de datos a través de las fronteras

Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección del debido tratamiento de datos personales, la información debe poder circular tan libremente como en el interior de cada uno de los territorios de que se trate.

Cuando no se ofrezcan garantías suficientes, no se podrán imponer limitaciones injustificadas a la circulación de información, sino solo en la medida en que así lo exija la protección de los derechos humanos.

Para determinar si un país cuenta con garantías comparables, se podrán evaluar, entre otros, los siguientes elementos:

a) La vigencia del estado de derecho; el respeto de los derechos humanos y las libertades fundamentales; y la legislación pertinente, tanto general como sectorial, sobre tratamiento de datos personales.

b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, con poderes de ejecución adecuados, y poderes para asistir y asesorar a los titulares de los datos, y cooperar con las autoridades de protección de datos.

c) Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

- Cuando se acredite que en el país o parte de su territorio, el sector, la actividad o la organización internacional destinatarios de los datos personales se cuenta con garantías comparables para asegurar el debido tratamiento de los datos personales, conforme a la legislación nacional del país desde donde se exportan los datos.
- Cuando el exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares de los datos. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional.
- Cuando el exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado por la autoridad de datos del país desde donde se envían los datos personales.
- Cuando el titular de los datos o la autoridad de control del país del exportador autorice la transferencia, según la legislación nacional que resulte aplicable en la materia.

Otras excepciones que los países autoricen a través de leyes o instrumentos internacionales.

23. Recolección internacional de datos personales

Los Estados adoptarán medidas apropiadas, útiles y oportunas para garantizar el debido tratamiento de los datos personales y la protección efectiva de los derechos de las personas cuya información recolecten los responsables o encargados ubicados en un país diferente al del domicilio o residencia del titular de los datos personales y que no tengan sede física o establecimiento en el país de domicilio o residencia del titular (recolector internacional de datos).

Además, los Estados cooperarán entre sí, con las autoridades de protección de datos y con los titulares de los datos para garantizar el objetivo señalado en el párrafo anterior.

El hecho de que el recolector internacional de datos no esté presente o no tenga residencia física o establecimiento en el país del titular de los datos no debe generar o facilitar impunidad o falta de protección de los derechos de las personas.

24. Campo de aplicación

Estos principios deberán aplicarse, en primer lugar, a todo tratamiento de datos personales, tanto públicos como privados, con independencia de los medios o tecnologías que se utilicen para ello.

B. Aplicación de los principios rectores al tratamiento de datos personales por parte de las organizaciones internacionales gubernamentales

Las organizaciones internacionales gubernamentales aplicarán estos principios rectores al tratamiento de datos personales, a reserva de las adaptaciones que sean necesarias para tener en cuenta las diferencias que podrían existir entre los ficheros o sistemas de información con fines internos, como los relativos a la gestión del personal, y los ficheros o sistemas de información con fines externos relativos a terceras personas relacionadas con la organización.

Cada organización deberá designar a la autoridad que, según su estatuto, sea competente para velar por la correcta aplicación de estos principios.

Cláusula humanitaria

Los Estados adoptarán medidas especiales sobre el tratamiento de datos personales para facilitar y apoyar acciones humanitarias con el objetivo de proteger y asistir a las personas vulnerables en el contexto de los conflictos armados, situaciones de violencia, situaciones de emergencia o desastres naturales.