RESOLUCIÓN SPSP-XXX-XXX-XXX

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que el numeral 2 del artículo 11 de la Constitución de la República del Ecuador ("CRE") establece: *"Art. 11.- El ejercicio de los derechos se regirá por los siguientes principios: **2.** Todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades. Nadie podrá ser discriminado por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural, estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física; ni por cualquier otra distinción, personal o colectiva, temporal o permanente, que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de los derechos. La ley sancionará toda forma de discriminación. El Estado adoptará medidas de acción afirmativa que promuevan la igualdad real en favor de los titulares de derechos que se encuentren en situación de desigualdad.";*

Que el numeral 8 del artículo 11de la CRE menciona lo siguiente: "*Art. 11.- El ejercicio de los derechos se regirá por los siguientes principios: (...) **8**. El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio. Será inconstitucional cualquier acción u omisión de carácter regresivo que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos.";*

Que el numeral 19 del artículo 66 de la CRE menciona que: *"[e]l derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley";*

Que el artículo 92 de la CRE menciona que: *"[t]oda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos(...)";*

Que el artículo 1 de la Ley Orgánica de Protección de Datos Personales ("LOPDP"), publicada en el Suplemento del Registro Oficial No. 459 del 26 de mayo de 2021, menciona: *"[e]l objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.";*

Que el artículo 2 de la LOPDP establece que la ley: *"se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso(...)";*

Que el artículo 3 de la LOPDP define el ámbito de aplicación territorial: *"[s]in perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando:**1.** El tratamiento de datos personales se realice en cualquier parte del territorio nacional; **2.** El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional; **3.** Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: 1) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador; y, **4.** Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.";*

Que el artículo 10 de la LOPDP establece que: *"[s]in perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de:**a) Juridicidad.-** Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable. **b) Lealtad.-**El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados. En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales. **c) Transparencia.-**El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia. **d) Finalidad.-**Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular: no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. e**) Pertinencia y minimización de datos personales.-**Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. **f)***

Proporcionalidad del tratamiento.-*El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos.* ***g) Confidencialidad.-****El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.* ***h) Calidad y exactitud.-*** *Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales. Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: a) Hubiesen sido obtenidos por el responsable directamente del titular. b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable. c) Fuesen obtenidos de un registro público por el responsable.* ***i) Conservación.-****Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento. Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.* ***j) Seguridad de datos personales.-****Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.* ***k) Responsabilidad proactiva y demostrada.-****El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento. El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales. El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.* ***l) Aplicación***

favorable al titular.-*En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.* ***m) Independencia del control.-****Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.";*

Que el artículo 20 de la LOPDP reconoce el derecho del titular a: *"(...) no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:* ***a.*** *Solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales:* ***b.*** *Presentar observaciones;* ***c.*** *Solicitar los criterios de valoración sobre el programa automatizado; o,* ***d.*** *Solicitar al responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos;* ***e.*** *Impugnar la decisión ante el responsable o encargado del tratamiento No se aplicará este derecho cuando:****1.*** *La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales;* ***2.*** *Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o,* ***3.*** *Se base en el consentimiento explícito del titular.* ***4.*** *La decisión no conlleve impactos graves o riesgos verificables para el titular. No se podrá exigir la renuncia a este derecho en forma adelantada a través de contratos de adhesión masivos. A más tardar en el momento de la primera comunicación con el titular de los datos personales, para informar una decisión basada únicamente en valoraciones automatizadas, este derecho le será informado explícitamente por cualquier medio idóneo.";*

Que el artículo 1 del Reglamento General de la Ley Orgánica de Protección de Datos Personales ("RGLOPDP"), expedido mediante Decreto Ejecutivo No. 904 y publicado en el Suplemento del Registro Oficial No. 435 del 13 de noviembre de 2023, señala que su objeto es: *"(...) desarrollar la normativa para la aplicación de la Ley Orgánica de Protección de Datos Personales y la protección de los derechos y libertades fundamentales de los titulares de datos personales.";*

Que el artículo 29 del RGLOPDP establece que la evaluación de impacto: *" (...) consiste en un análisis preventivo, de naturaleza técnica, mediante el cual el responsable valora los impactos reales del tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con el cumplimiento de los principios y el respeto de los derechos y de las obligaciones establecidas en la Ley Orgánica de Protección de Datos Personales, este Reglamento y demás normativa aplicable.";*

Que el artículo 58 del RGLOPDP establece que: *"[e]l responsable del tratamiento está obligado a aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos que realiza es conforme con la*

normativa. Para ello se deberá atender: ***1.*** *La naturaleza;* ***2.*** *El ámbito;* ***3.*** *La finalidad del tratamiento; y,* ***4.*** *Los riesgos. Esta obligación implica también revisar y actualizar las medidas cuando sea necesario.";*

Que el artículo 59 del RGLOPDP menciona que*: "[e]l responsable del tratamiento tiene la obligación de establecer medidas técnicas y organizativas adecuadas para aplicar los principios establecidos en la normativa de forma eficaz, y proteger los derechos de los titulares, de manera previa al tratamiento de datos personales. Para la fijación de estas medidas debe tenerse en cuenta:* ***1.*** *La naturaleza, ámbito y finalidad del tratamiento;* ***2.*** *Los riesgos de diversa probabilidad y gravedad asociados al tratamiento;* ***3.*** *El estado de la técnica; y,* ***4.*** *El coste de aplicación.";*

Que el artículo 60 del RGLOPDP establece que: *"[e]l responsable del tratamiento adoptará las medidas técnicas y organizativas apropiadas para garantizar que, mediante ajustes, por defecto, solo puedan tratarse aquellos datos personales cuyo tratamiento sea necesario para la respectiva finalidad específica del tratamiento. Además, mediante los respectivos ajustes, las medidas deben garantizar que, por defecto, los datos no puedan ser accesibles a un número indefinido de personas de forma automatizada. Esta obligación es aplicable a:* ***1.*** *La cantidad de los datos recopilados;* ***2.*** *La extensión del tratamiento;* ***3.*** *El período de almacenamiento; y,* ***4.*** *La accesibilidad. Para acreditar el cumplimiento de esta medida, podrá utilizarse un mecanismo de certificación, según lo previsto en la Ley Orgánica de Protección de Datos Personales.";*

Que en junio 03 de 2024 se admitió de manera unánime a la Superintendencia de Protección de Datos Personales como *"miembro de pleno derecho de la RIPD, con voz y voto",* en este sentido se constituye en una referencia técnica y jurídica por lo que se hace referencia a los *"Estándares de Protección de Datos Personales para los Estados Iberoamericanos"***,** aprobados por la Red Iberoamericana de Protección de Datos (RIPD**),** los cuales constituyen una referencia técnica y jurídica para el desarrollo de normativas de protección de datos en la región, e instan a incorporar garantías reforzadas para los tratamientos automatizados que puedan afectar derechos fundamentales, en este sentido también se emitieron las *"Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial"* documento aprobado por las entidades integrantes de la RIPD **e**n la sesión del 21 de junio de 2019 llevada a cabo en la ciudad de Naucalpan de Juárez, México;

Que la Recomendación sobre la Ética de la Inteligencia Artificial adoptada por la UNESCO en 2021 y el documento *"Hacia una regulación ética y efectiva de la Inteligencia Artificial en Ecuador. Recomendaciones para una Ley de IA en el país***"** elaborado por la UNESCO y publicado en 2025, exhortan a los Estados a establecer marcos normativos que aseguren la protección efectiva de los derechos humanos frente al uso de tecnologías algorítmicas, incluyendo los principios de transparencia, explicabilidad, trazabilidad, supervisión humana y prevención de sesgos;

Que el Informe "*Panorama de la Inteligencia Artificial en América Latina y el Caribe 2025"*, elaborado conjuntamente por el Programa de las Naciones Unidas para el Desarrollo (PNUD) y la Alianza Latinoamericana de Inteligencia Artificial (AILA), recomienda a los Estados implementar mecanismos nacionales de gestión de riesgos en inteligencia artificial, clasificando

los sistemas según su nivel de riesgo y aplicando medidas diferenciadas de evaluación, mitigación y seguimiento, en especial cuando se involucre el tratamiento de datos personales;

Que conforme lo expuesto, resulta necesario establecer un instrumento normativo que regule sistemas de inteligencia artificial que, directa o indirectamente, involucren el tratamiento de datos personales, a fin de garantizar la protección efectiva de los derechos y libertades fundamentales de los titulares, en observancia de los principios de licitud, lealtad, transparencia, confidencialidad, minimización, proporcionalidad, responsabilidad proactiva y seguridad desde el diseño y por defecto, conforme lo dispuesto en la Ley Orgánica de Protección de Datos Personales, su Reglamento General y los estándares internacionales aplicables;

Que en concordancia con lo previamente mencionado, la adopción de referencias internacionales como las recomendaciones de la RIPD, la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO, permite dotar de coherencia técnica y legitimidad normativa al marco regulatorio nacional, asegurando su compatibilidad con estándares ampliamente aceptados en el ámbito regional y global. Estas referencias constituyen instrumentos orientadores que facilitan la aplicación de los principios de protección de datos en entornos automatizados, y refuerzan la interpretación sistemática de los derechos del titular frente al uso de tecnologías emergentes;

Que además, las directrices previamente referidas ofrecen lineamientos para la evaluación de impacto, la gestión del riesgo algorítmico, la supervisión humana significativa y el uso responsable de datos, aspectos esenciales en el diseño y despliegue de sistemas de inteligencia artificial. Su incorporación en la presente normativa fortalece la capacidad de anticipación del Estado frente a posibles afectaciones a los derechos fundamentales, promueve una cultura de gobernanza tecnológica responsable y fomenta la interoperabilidad jurídica con otras jurisdicciones, en beneficio de la seguridad jurídica, la cooperación internacional y la protección efectiva de los datos personales en el ecosistema digital;

Que la IRD, a través del informe técnico **Nº INF-SPDP-IRD-2025-0069** del 29 de agosto de 2025, justificó la pertinencia y la necesidad de emitir la norma que regula el tratamiento de datos personales en sistemas de inteligencia artificial; informe técnico que, en su parte pertinente, señala: *"[l]a SPDP en ejercicio de sus funciones y atribuciones está facultada de conformidad con el numeral 5 del artículo 76 de la LOPDP para emitir el Reglamento para la Garantía del Derecho de Protección de Datos Personales en el Uso de Inteligencia Artificial."*; y, recomendó: *"(...) iniciar con el proceso de socialización del proyecto de Reglamento para la garantía del derecho de protección de datos personales en el uso de inteligencia artificial, en cumplimiento con lo dispuesto por la Resolución N° SPDP-SPDP-2024-0022-R para que en el término de veinte (20) días la ciudadanía pueda realizar sus aportes.";*

Que por medio del memorando **N° SPDP-IRD-2025-0163-M,** suscrito el 29 de agosto de 2025, la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") tanto el proyecto normativo denominado **Normativa General para la Garantía del Derecho de Protección de Datos Personales en el Uso De Inteligencia Artificial,** como el informe técnico **N° INFSPDP- IRD-2025-0069,** para que, dentro del término de diez días, se pronuncie sobre la concordancia con la normativa y la legalidad, de conformidad con lo dispuesto en la resolución N° SPDP-SPDP-2024-0022-R del 31 de diciembre del 2024, que contiene el

Reglamento para la Creación, Modificación y Derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales, publicado en el Registro Oficial N° 734 del 31 de enero del 2025;

Que a través del informe jurídico **N° INF-SPDP-DAJ-2025-0040,** remitido a la IRD mediante memorando **N° SPDP-DAJ-2025-0073-M** suscrito el **29 de agosto** de **2025,** la DAJ determinó que el **Normativa General para la Garantía del Derecho de Protección de Datos Personales en el Uso De Inteligencia Artificial,** es congruente con los principios establecidos en la LOPDP, por cuanto no transgrede o contradice normas matrices, cumple con el principio de legalidad y, por ello, recomendó que *"(...)[l]a IRD debe solicitar a quien corresponda la publicación a través de la página web institucional e informar su publicación a través de las redes sociales institucionales, con la finalidad de que la ciudadanía, las organizaciones de la sociedad civil o interesados en general, de manera motivada, puedan remitir sus observaciones o realizar aportes respecto del contenido (...)"*;

Que mediante el memorando **N° SPDP-IRD-2025-0164** suscrito el 29 de agosto de 2025, la IRD solicitó a las unidades administrativas de la SPDP que procedan con las acciones pertinentes, a fin de que publiquen el borrador de la **Normativa General para la Garantía del Derecho de Protección de Datos Personales en el Uso De Inteligencia Artificial,** en la página web institucional y en las redes sociales de la SPDP, para que el proyecto de normativa esté disponible para la ciudadanía, las organizaciones de la sociedad civil o los interesados en general desde el **02 al 29 de septiembre del 2025,** inclusive, con el objeto de poder recibir sus observaciones o aportes, siempre que estuvieren debidamente motivados;

Que para cumplir con la resolución Nº SPDP-SPDP-2024-0022-R, se ejecutó el proceso de socialización del Proyecto de **Normativa General para la Garantía del Derecho de Protección de Datos Personales en el Uso De Inteligencia Artificial**, dentro del término de veinte días, de conformidad con el artículo 12 de dicha resolución; y, como resultado de ese proceso, se XXXXXX**;**

Que a través del informe técnico Nº **INF-SPDP-IRD-2025-00XXX,** la IRD incorporó las observaciones y aportes que se consideraron relevantes y adecuados, previa justificación de las modificaciones realizadas al proyecto normativo;

EN EJERCICIO de sus atribuciones constitucionales, legales y reglamentarias,

RESUELVE:

NORMATIVA GENERAL PARA LA GARANTÍA DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN EL USO DE INTELIGENCIA ARTIFICIAL

CAPÍTULO I.- DISPOSICIONES GENERALES

Artículo 1. Objeto: El presente Reglamento tiene por objeto establecer los principios, obligaciones que deben observar los responsables y encargados del tratamiento de datos

personales cuando se utilicen sistemas de inteligencia artificial que involucren el tratamiento de datos personales.

Artículo 2. Ámbito de aplicación: Este Reglamento es aplicable a todos los responsables y encargados del tratamiento de datos personales, que a la vez sean proveedores, entrenadores y/o desplegadores de sistemas de inteligencia artificial de acuerdo con lo previsto en el ámbito territorial de la Ley Orgánica de Protección de Datos Personales.

Artículo 3.- Definiciones: Para efectos del presente Reglamento se aplicarán, en complemento con las definiciones de la Ley Orgánica de Protección de Datos Personales y su Reglamento General, las siguientes:

1. Deepfake: Técnica basada en inteligencia artificial, que permite crear o alterar imágenes, audios o videos de forma altamente realista para simular, de manera falsa, que una persona ha dicho o hecho algo que no ha ocurrido.
2. Explicabilidad algorítmica: Capacidad de una persona para comprender cómo y por qué un sistema de inteligencia artificial llegó a una decisión.
3. Sistema de inteligencia artificial: Es la tecnología basada en máquinas diseñada para operar con distintos niveles de autonomía y capacidad de adaptación después de su implementación. Para alcanzar objetivos explícitos o implícitos, analiza la información de entrada y genera resultados como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.
4. Desplegador: una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional;
5. Comercialización: el suministro de un sistema de IA o de un modelo de IA de uso general para su distribución o utilización en el mercado, en el transcurso de una actividad comercial, previo pago o gratuitamente;
6. Distribuidor: una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA
7. Datos de entrenamiento: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables;
8. Datos de validación: los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el subajuste o el sobreajuste;
9. Datos de calibración. Los modelos utilizados para estimar un intervalo de confianza tanto en modelos de clasificación, como de regresión,
10. Datos de prueba: los datos usados para proporcionar una evaluación independiente del sistema de IA, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio.
11. Datos sintéticos: Los datos generados de manera artificial con el fin de entrenar a un sistema de IA.
12. Sistema de identificación biométrica remota en tiempo real: un sistema de identificación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas

13. Espacio de acceso público: cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad
14. Minería de datos: Proceso computacional que extrae patrones mediante el análisis de datos cuantitativos desde diferentes perspectivas y dimensiones, categorizándolos y resumiendo las posibles relaciones e impactos.
15. Sistema experto: Sistema de IA que acumula, combina y encapsula el conocimiento proporcionado por uno o varios expertos humanos en un ámbito específico para inferir soluciones a problemas.
16. Modelo: Representación física, matemática o lógica de un sistema, entidad, fenómeno, proceso o datos.
17. IA específica: Tipo de sistema de IA que se centra en tareas definidas para abordar un problema específico.
18. IA General: Inteligencia artificial general del sistema de IA. Tipo de tarea que aborda una amplia gama de con un nivel satisfactorio de rendimiento
19. Conjunto de datos: Recopilación de datos con un formato compartido.
20. Datos de evaluación: Datos utilizados para evaluar el rendimiento de la formación de un modelo de datos final.
21. Aprendizaje automático: Proceso de optimización de los parámetros del modelo mediante técnicas computacionales, de modo que el comportamiento del modelo refleje los datos o la experiencia.
22. Modelo de aprendizaje automático: Construcción matemática que genera una inferencia o predicción basada en datos de entrada o información
23. Entrenamiento del modelo: Proceso para determinar o mejorar el intervalo de acierto de un modelo, basado en datos de entrenamiento.
24. Modelos de lenguaje largo (LLM): son modelos de aprendizaje profundo muy grandes que se preentrenan con grandes cantidades de datos. El transformador subyacente es un conjunto de redes neuronales que consta de un codificador y un decodificador con capacidades de autoatención
25. Aprendizaje profundo: Es un subconjunto del aprendizaje automático es un campo de la inteligencia artificial (IA) que se centra en el uso de redes neuronales artificiales con muchas capas (profundas) para analizar datos y aprender patrones complejos
26. IA generativa: es un tipo de inteligencia artificial capaz de crear contenido nuevo y original, como texto, imágenes, música, audio y vídeo
27. IA Agentica: sistemas de inteligencia artificial diseñados para funcionar de forma autónoma, tomando decisiones y emprendiendo acciones para alcanzar objetivos específicos con una intervención humana mínima.
28. *Retrieval Augmented Generation*: RAG mejora los modelos de lenguaje grande (LLM) al proporcionarles acceso a una base de conocimientos externa (como una base de datos o un conjunto de documentos) para recuperar información relevante antes de generar una respuesta.
29. Bases de datos vectoriales: es un sistema de gestión de datos diseñado para almacenar, gestionar y consultar incrustaciones vectoriales, que son representaciones numéricas de datos no estructurados como texto, imágenes o audio

CAPÍTULO II: PRINCIPIOS RECTORES Y GARANTÍAS EN EL USO DE INTELIGENCIA ARTIFICIAL

Artículo 4.- Principios aplicables: Los sistemas de inteligencia artificial que impliquen tratamiento de datos personales deberán regirse, a más de los ya establecidos en la Ley Orgánica de Protección de Datos Personales, en los siguientes:

1. Transparencia: De acuerdo con el principio de transparencia reconocido en el literal c del artículo 10 de la Ley Orgánica de Protección de Datos Personales, el tratamiento de datos personales en los sistemas de inteligencia artificial, desde su diseño, deberá ser transparente, fácil entender y deberán comunicarse al titular de los datos personales con un lenguaje sencillo y claro para fácil comprensión.
2. Responsabilidad: El responsable y encargado del tratamiento de datos personales que implemente sistemas de inteligencia artificial en o para cualquier tratamiento de datos personales, es responsable absoluto de dichos datos y en caso de que haya una vulneración se aplicará el numeral 1 del artículo 68 y 70 de la Ley Orgánica de Protección de Datos Personales.
3. Confidencialidad: Todo sistema de inteligencia artificial que involucre datos personales deberá proteger la confidencialidad de los mismos en todas sus etapas de acuerdo con lo establecido en la Ley Orgánica de Protección de Datos Personales.
4. Supervisión humana significativa: Es una buena práctica que se aplica en todo sistema automatizado el cual debe permitir intervención humana que pueda revisar, revertir o validar decisiones que afecten derechos fundamentales.
5. Seguridad desde el diseño y por defecto: los sistemas de inteligencia artificial deben incorporar medidas de seguridad técnicas y organizativas desde su concepción, minimizando los riesgos de vulneración de la seguridad de datos personales.
6. Protección de datos personales desde el diseño y por defecto. Se deben implementar en los sistemas de inteligencia artificial, estrategias y operaciones para minimizar, ocultar, separar, abstraer, informar, controlar, cumplir y demostrar, la protección de los datos personales de los titulares. La implementación deberá realizarse en todas las etapas de entrenamiento, calibración, testeo y despliegue de los sistemas de inteligencia artificial.

Artículo 5.- Derechos de los titulares frente al uso de sistemas de inteligencia artificial: Los titulares de datos personales gozan de todos los derechos reconocidos en la Ley Orgánica de Protección de Datos Personales, especialmente de los siguientes derechos específicos cuando sus datos sean objeto de tratamiento mediante sistemas de inteligencia artificial:

1. Derecho a conocer si están siendo evaluados por decisiones totalmente automatizadas, esto quiere decir que el titular de datos personales podrá solicitar esta información en cualquier momento.
2. Derecho a la información de acuerdo con el numeral 17 del artículo 12 de la Ley Orgánica de Protección de Datos Personales, por el cual el titular de datos personales también puede solicitar información respecto al sistema de inteligencia artificial el cual se use para realizar un tratamiento de datos personales.
3. Derecho a oponerse a tratamientos de datos personales que emitan decisiones automatizadas que generen consecuencias desproporcionadas, discriminatorias o no justificadas frente al titular de datos personales.

CAPÍTULO III: OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS

Artículo 6.- Obligaciones de los responsables y encargados del tratamiento en el uso de inteligencia artificial: Los responsables y encargados del tratamiento de datos personales que utilicen sistemas de inteligencia artificial deberán cumplir con las siguientes obligaciones específicas:

1. Informar de manera clara, específica y transparente al titular de datos personales respecto al tratamiento que se llevará a cabo mediante sistemas de inteligencia artificial, incluyendo las finalidades del tratamiento y su carácter automatizado.
2. Implementar procedimientos para garantizar la intervención humana cuando los sistemas de inteligencia artificial puedan generar efectos jurídicos o impactar a los derechos del titular.
3. Auditar adecuadamente el funcionamiento general del sistema de inteligencia artificial, cuando realice actividades de tratamiento de datos personales.
4. En caso de incluir datos personales para realizar pruebas de sistemas de inteligencia artificial, los atributos de la identidad de personas naturales deberán ser obfuscados de tal modo que no permitan la identificación del titular de manera directa.
5. Realizar la correspondiente gestión de riesgos y evaluaciones de impacto del tratamiento de datos personales, de acuerdo con la normativa específica emitida por la Superintendencia de Protección de Datos Personales,
6. Garantizar la trazabilidad del uso de los datos personales dentro del sistema de inteligencia artificial y mantener registros accesibles para auditoría por parte de la Superintendencia de Protección de Datos Personales.
7. Cuando se realice un tratamiento de datos personales mediante sistemas de inteligencia artificial se deberá incluir en el Registro de Actividades de Tratamiento que el mencionado tratamiento usa en dichos sistemas.

Artículo 7.- Análisis de gestión de riesgos y evaluación de impacto: El responsable o encargado del tratamiento antes de poner en funcionamiento o utilizar un sistema de inteligencia artificial que implique el tratamiento de datos personales, deberá realizar una gestión de riesgos y evaluación de impacto de acuerdo con lo establecido en los artículos 40, 41 y 42 de la LOPDP, para cada tratamiento de datos personales que involucre sistemas de inteligencia artificial, de manera obligatoria.

Artículo 8.- Auditoría y trazabilidad algorítmica: Los responsables y encargados del tratamiento de datos personales deberán implementar mecanismos técnicos, administrativos, organizativos y jurídicos que garanticen la trazabilidad, supervisión y auditoría de los sistemas de inteligencia artificial, especialmente aquellos que conlleven un mayor riesgo para la protección de datos personales. Estos mecanismos deberán permitir:

1. Llevar bitácoras de las decisiones automatizadas derivadas del tratamiento de datos personales, las cuales deberán estar disponibles para auditorías internas y para la Superintendencia de Protección de Datos Personales.
2. Realizar auditorías técnicas y éticas periódicas sobre los modelos, fuentes de datos, patrones de entrenamiento y desempeño algorítmico.
3. Identificar sesgos en los conjuntos de datos utilizados para entrenar al sistema.

4. Corregir y procurar equiparar los sesgos detectados, con el fin de entrenar el sistema de inteligencia artificial de la manera más neutral posible, cuando se trate de sistemas de inteligencia artificial que tomen decisiones totalmente automatizadas que pudiesen vulnerar los derechos y libertades de los titulares de datos.

CAPÍTULO IV: USOS NO PERMITIDOS

Artículo 9.- Prohibiciones del uso de datos personales en sistemas de inteligencia artificial: Por considerarse lesivos a los derechos fundamentales de los titulares de datos personales, se prohíbe el despliegue, entrenamiento implementación, comercialización o uso de sistemas de inteligencia artificial en los siguientes casos:

1. Los sistemas de identificación biométrica remota en tiempo real en espacios públicos, salvo en los casos expresamente autorizados por norma con rango de ley o bajo control judicial. Los sistemas de identificación biométrica en espacios privados, pero de acceso público tales como el ingreso a edificios de oficinas, hospitales, urbanizaciones, deberán conformarse a los establecido en el artículo 9 del Reglamento. La SPDP podrá auditar en cualquier momento los sistemas de identificación biométrica en espacios privados, y emitir como medida cautelar el cese de funcionamiento de ellos, cuando no cumplan con la legitimidad del tratamiento, el ejercicio de derechos de los titulares de datos personales, la gestión de riesgos y evaluación de impacto del tratamiento de datos personales, y demás obligaciones establecidas en la LOPDP, el RLPDP, y la normativa vigente emitidas por la SPDP.
2. Sistemas que generen o difundan contenidos falsificados que utilicen datos personales, incluidos los denominados *deepfakes*,

DISPOSICIÓN FINAL

Esta resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dada y firmada en Quito, D. M., el XXX del 2025.

FABRIZIO PERALTA-DÍAZ

SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES