Secretaría General Iberoamericana

Secretaria-Geral Ibero-Americana

RED IBEROAMERICANA DE PROTECCION DE DATOS

ACTUALIZACIÓN DE LOS ESTÁNDARES DE PROTECCIÓN DE DATOS DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS, EN EL MARCO DE LA IMPLEMENTACIÓN DE LA CIPDED

INFORME FINAL

NELSON REMOLINA ANGARITA

2025

CON EL APOYO DE

Cooperación Española

1. Las opiniones expresadas son responsabilidad exclusiva del autor, sin que comprometa ni refleje necesariamente los puntos de vista de la SEGIB o sus países miembros.

Actualización de los estándares de protección de datos de la Red Iberoamericana de protección de datos, en el marco de la implementación de la CIPDED

Informe final

Nelson Remolina Angarita[1]

[1] Las opiniones expresadas son responsabilidad exclusiva del autor, sin que comprometa ni refleje necesariamente los puntos de vista de la SEGIB o sus países miembros.

Con el apoyo de:

Con el apoyo de:

Cooperación Española

Tabla de contenido

Siglas *8*

Glosario *9*

Mapas y tablas *11*

Mapas 11

Tablas 11

Gráficas 12

Introducción *12*

Del derecho a la protección de datos en la Carta de los Derechos Fundamentales de la Unión Europea y la autodeterminación informativa en la Corte Interamericana de Derechos Humanos (CIDH). *14*

Necesidad de modernizar las regulaciones para garantizar el debido tratamiento de los datos personales y los derechos humanos en una sociedad digital *17*

Propuesta de Global Privacy Assembly -GPA- (2023) 18

Propuesta de actualización de la ONU (2024) 21

Propuesta de una Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales (2024) 23

La protección de datos personales en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales *28*

Principio1: Centralidad de las personas. Derechos y deberes en entornos digitales. 29

Principio 3: Privacidad, confianza, seguridad de datos y ciberseguridad 30

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Principio 5: Especial atención a niñas, niños y adolescentes 31

Principio 9: Un abordaje de las tecnologías emergentes que no renuncie a la centralidad de las personas 32

Análisis comparativo de documentos internacionales sobre tratamiento de datos personales 32

Principios sobre el tratamiento de datos personales en documentos internacionales 37

Derechos de las personas respecto del tratamiento de datos personales en documentos internacionales 42

Medidas proactivas para el debido tratamiento de datos personales en documentos internacionales 46

Alternativas para realizar transferencias internacionales de datos personales 47

Características que deben tener las autoridades de protección de datos personales 49

Algunos aspectos sobre protección de datos personales en las constituciones de los países miembros de la SEGIB 53

Análisis comparativo de las regulaciones sobre tratamiento de datos personales en los países miembros de la SEGIB 57

Principios sobre el tratamiento de datos personales en la regulación de los países miembros de la SEGIB. 58

Derechos de las personas respecto del tratamiento de datos personales en la regulación de los países miembros de la SEGIB 60

Medidas proactivas para el debido tratamiento de datos personales en la regulación de los países miembros de la SEGIB 62

Alternativas para realizar transferencias internacionales de datos personales en la regulación de los países miembros de la SEGIB. 64

Características que deben tener las autoridades de protección de datos personales según la regulación de los países miembros de la SEGIB 66

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Desafíos derivados de las neurotecnologías, la inteligencia artificial y el internet de las cosas respecto del tratamiento de datos personales 68

Desafíos comunes o generales de las neurotecnologías, la inteligencia artificial y el internet de las cosas respecto del tratamiento de datos personales 69

Desafíos de las neurotecnologías 70

Desafíos de la inteligencia artificial (IA) 76

Algunos lineamientos del Reglamento Europeo de Inteligencia Artificial (REIA) 81

Prácticas prohibidas 82

Evaluación de impacto relativa a los derechos fundamentales y derecho de explicabilidad 85

Desafíos en torno a la protección de los menores en entornos digitales con relación al tratamiento de los datos personales 87

Del anteproyecto de ley del Reino de España para la protección de las personas menores de edad en los entornos digitales 94

Desafíos a tener en cuenta al momento de crear o fortalecer las autoridades nacionales de protección de datos en los países iberoamericanos..... 102

PROPUESTAS..... 105

Propuesta de actualización de los estándares iberoamericanos para promover el fortalecimiento de la protección de los datos personales en el marco de las tecnologías emergentes, así como su uso ético y responsable. 105

¿En qué consisten las modificaciones? 111

Propuestas sobre Autoridades de Protección de Datos (APD) 113

Propuestas sobre Neurotecnologías 115

Propuestas sobre Inteligencia Artificial 117

Propuestas sobre protección de los menores de edad en entornos digitales 117

Texto de las modificaciones sugeridas 118

Propuesta para proteger los niños, las niñas y los adolescentes frente a los desafíos de la sociedad digital. 128

Propuesta respecto de neurotecnologías..... 131

Con el apoyo de:
Con el apoyo de:
Cooperación Española

ANEXOS 137

Anexo 1 : Propuesta de ley modelo mediante la cual se regulan principios en materia de neurociencias, neurotecnologías y derechos humanos 137

Anexo 2 : Propuesta de Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales..... 148

Anexo 3 : Listado de documentos sobre protección de datos, neurotecnologías e inteligencia artificial y derechos digitales emitidos por organizaciones internacionales y autoridades de protección de datos 182

Agencia Española de Protección de Datos (AEPD) 182
Asia-Pacific Economic Cooperation (APEC) 182
Organización de las Naciones Unidas (ONU) 182
Comisión Europea (CE) 183
Consejo de Europa (CdE) 184
Global Privacy Assembly (GPA) 185
Grupo de trabajo sobre protección de datos del artículo 29 186
Comité Europeo de Protección de Datos (CEPD) 186
Organización de Estados Americanos (OEA) 187
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) 188
Organización para la Cooperación y el Desarrollo Económico (OCDE). 188
Parlamento Europeo (PE) 189
Parlamento Latinoamericano y Caribeño (PLC) 190
Red Iberoamericana de protección de datos (RIPD) 190
Secretaría General Iberoamericana (SEGIB) 190
Superintendencia de Industria y Comercio (SIC). Delegatura para la protección de datos personales 190
Unión Europea (UE) 191

Anexo 4. Principales normas constitucionales y legales sobre regulación de tratamiento de datos personales en los países miembros de la SEGIB 191

Andorra 192
Argentina 192
Bolivia 192
Brasil 192
Costa Rica 192

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Cuba 193
Chile 193
Colombia 194
Ecuador 195
El Salvador 195
España 196
Guatemala 196
Honduras 197
México 197
Nicaragua 198
Panamá 198
Paraguay 198
Perú 199
Portugal 199
República Dominicana 200
Uruguay 200
Venezuela 201

Anexo 5. Proyectos de ley sobre Protección de Datos en la región Iberoamericana y otras iniciativas relevantes extra regionales. 201

Argentina 202

Bolivia 203

Colombia 204

Costa Rica 208

Honduras 208

República Dominicana 209

Anexo 6: Identificación de buenas prácticas y experiencias comparadas en el tratamiento de datos personales. 210

Creación de canales prioritarios para casos especiales o para la protección de los datos personales de las niñas, los niños y los adolescentes (NNA). 213

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Promover la sensibilización sobre la protección de datos entre los NNA 215

Continuar educando a la población sobre el derecho de protección de datos..... 215

Facilitar herramientas para facilitar y demostrar cumplimiento de la regulación sobre tratamiento de datos 216

Ayuda a las pymes para cumplir la regulación 217

Crear herramientas digitales para el ejercicio de los derechos ante los responsables del tratamiento y la autoridades de protección de datos 218

Creación de mecanismos voluntarios y alternativos de solución de controversias sobre tratamiento de datos (experiencia del caso SICFACILITA de la República de Colombia) 218

Anexo 7. Algunas políticas públicas sobre tratamiento de datos personales en los países miembros de la SEGIB 236

Anexo 8. Elementos iniciales para establecer la la eficacia y operabilidad de los marcos normativos de los países iberoamericanos y potencial coordinación entre ellos. 238

Eficacia y operabilidad de los marcos normativos de los países Iberoamericanos..... 238

Anexo 9. Viabilidad de la potencial coordinación entre los marcos normativos de los países Iberoamericanos 254

Siglas

AEPD : Agencia Española de Protección de Datos

Con el apoyo de:
Con el apoyo de:
Cooperación Española

APEC	:	Asia-Pacific economic Cooperation
CdE	:	Consejo de Europa
CE	:	Comisión Europea
CEPD	:	Comité Europeo de Protección de Datos
CNPD	:	Comisión Nacional de Protección de Datos (Portugal)
GTPD	:	Grupo de trabajo sobre protección de datos del artículo 29.
IA	:	Inteligencia Artificial
IoT	:	Internet de las Cosas (Internet of Things)
NGTDP	:	Normas generales sobre tratamiento de datos personales
NNA	:	Niñas, niños y adolescentes
OCDE	:	Organización para la Cooperación y el Desarrollo Económico
OEA	:	Organización de Estados Americanos
ONU	:	Organización de las Naciones Unidas
PE	:	Parlamento Europeo
PLC	:	Parlamento Latinoamericano y Caribeño
REIA	:	Reglamento Europeo de Inteligencia Artificial
RIPD	:	Red Iberoamericana de protección de datos
SEGIB	:	Secretaría General Iberoamericana
SIC	:	Superintendencia de Industria y Comercio. Delegatura de protección de datos
UE	:	Unión Europea
UNESCO	:	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Glosario

Para los efectos del presente estudio hemos tomado como referencia las siguientes definiciones contenidas en los "Estándares de protección de datos personales para los países Iberoamericanos"[2] aprobados en 2017 por la Red Iberoamericana de protección de datos (RIPD).

[2] El texto de los estándares de la RIPD puede consultarse en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

- **Datos Personales**: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.
- **Datos personales sensibles**: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.
- **Encargado**: prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.
- **Exportador:** persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.
- **Responsable**: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
- **Titular:** persona física a quien le conciernen los datos personales.
- **Tratamiento**: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Mapas y tablas

Mapas

- Mapa 1. Disposiciones constitucionales y normas generales sobre tratamiento de datos personales en los países miembros de la SIGEB

Tablas

- Tabla 1. Principios sobre tratamiento de datos personales en documentos internacionales
- Tabla 2. Derechos de la persona titular del dato en documentos internacionales
- Tabla 3. Medidas proactivas para el tratamiento de datos personales en documentos internacionales
- Tabla 4. Alternativas para realizar transferencias internacionales de datos personales según documentos internacionales
- Tabla 5. Requisitos que expresamente exigen documentos internacionales sobre las autoridades de control o protección de datos personales
- Tabla 6. Principios sobre tratamiento de datos personales en las regulaciones de los países miembros de la SEGIB
- Tabla 7. Derechos de la persona titular del dato en la regulación de los países miembros de la SEGIB
- Tabla 8. Medidas proactivas para el tratamiento de datos personales en las regulaciones de los países miembros de la SEGIB
- Tabla 9. Alternativas para realizar transferencias internacionales de datos personales según las regulaciones de los países miembros de la SEGIB
- Tabla 10. Requisitos de las autoridades de control o protección de datos personales en las regulaciones de los países miembros de la SEGIB

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Gráficas

- Resumen de los aspectos generales de la propuesta de actualización de los estándares de la RIPD de 2017
- Propuesta para proteger los niños, las niñas y los adolescentes frente a los desafíos de la sociedad digital.

Introducción

En un entorno donde la tecnología avanza a un ritmo vertiginoso, la protección de los datos personales y los derechos de los menores en el mundo tecnológico son dos pilares esenciales no sólo para garantizar los derechos humanos en el entorno digital, sino para fijar las bases de una sociedad digital confiable, incluyente y centrada en el ser humano. Por un lado, innovaciones como las neurotecnologías y la inteligencia artificial plantean desafíos sin precedentes que exigen una respuesta clara para preservar la autodeterminación informativa, garantizar el debido tratamiento de los datos personales y la dignidad humana. Por otro lado, los niños, niñas y adolescentes, al ser especialmente vulnerables en el entorno digital, requieren una protección reforzada. El correcto tratamiento de sus datos y la garantía de sus derechos demandan regulaciones adecuadas que aseguren su bienestar en un mundo cada vez más interconectado.

Desde la proclamación de la Carta de los Derechos Fundamentales de la Unión Europea[3] en el año 2000, se ha subrayado la importancia de proteger los datos personales como un derecho autónomo e independiente. El artículo 8 de esta Carta, ha servido como una guía fundamental en la protección de la privacidad en la era digital. Paralelamente, la Corte Interamericana de Derechos Humanos (CIDH) ha reconocido la autodeterminación informativa como un derecho humano autónomo, esencial para salvaguardar otros derechos fundamentales. En su sentencia del 18 de octubre de

3 Cfr. PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, COMISIÓN EUROPEA. 2000. Carta de los derechos fundamentales de la Unión Europea. El texto oficial fue publicado en el Diario Oficial de las Comunidades Europeas C 364/7 del 18 de diciembre de 2000

Con el apoyo de:
Con el apoyo de:
Cooperación Española

2023, la CIDH resaltó la necesidad de que los Estados adopten mecanismos prácticos y eficaces para garantizar este derecho, destacando que su protección debe reflejarse en la implementación de prácticas concretas.

La protección de datos personales ha adquirido una relevancia central, impulsada por el desarrollo tecnológico y la creciente digitalización de las sociedades. En este contexto, los estándares iberoamericanos de protección de datos, aprobados en 2017 por la Red Iberoamericana de Protección de Datos (RIPD), representan un marco fundamental para garantizar los derechos de las personas en el ámbito digital dentro de la región. Estos estándares han servido como referencia para los países miembros, ofreciendo lineamientos comunes que facilitan la protección de los datos personales en consonancia con las mejores prácticas internacionales.

También es relevante destacar que las Jefas y los Jefes de Estado y de Gobierno de 22 países iberoamericanos aprobaron el 25 de marzo de 2023 la Carta Iberoamericana de Principios y Derechos en Entornos Digitales (CIPDED). Dentro de los diez (10) principios de la CIPDED, se mencionan algunos relacionados con el tratamiento de datos personales y las tecnologías emergentes, a saber: Centralidad de las personas. Derechos y deberes en entornos digitales. (principio 1); Privacidad, confianza, seguridad de datos y ciberseguridad. (principio 3); Especial atención a niñas, niños y adolescentes (principio 5); Un abordaje de las tecnologías emergentes que no renuncie a la centralidad de las personas (principio 9)

En este sentido, la CIPDED se posiciona como un catalizador clave para impulsar nuevas iniciativas en el ámbito iberoamericano, fomentando la creación y actualización de normativas que se adapten a los desafíos emergentes. La presente investigación y la propuesta de reforma de los estándares iberoamericanos son parte de este esfuerzo colectivo. Tanto la SEGIB como la RIPD han jugado un papel crucial en la promoción de estos esfuerzos, contribuyendo a la consolidación de un marco regional robusto que permita una protección efectiva y armonizada de los datos personales en toda la región y que garantice los derechos de los menores en el entorno digital.

Este estudio tiene como objetivo principal la elaboración de un análisis en el marco de la implementación de la Carta Iberoamericana de Principios y Derechos en Entornos Digitales (CIPDED) aprobada durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, 25 de marzo de 2023, y la elaboración de un documento que proponga lineamientos, estándares y otras

Con el apoyo de:
Con el apoyo de:
Cooperación Española

recomendaciones para el diseño e implementación de políticas públicas en materia de protección de datos para los países iberoamericanos, tomando como referencia los Estándares Iberoamericanos de Protección de Datos desarrollados por la Red Iberoamericana de Protección de Datos (RIPD) y alineándolos con los desafíos tecnológicos actuales.

Como parte del mismo, se hará referencia a los desafíos

(1) derivados de las neurotecnologías y la inteligencia artificial en materia de protección de datos personales.

(2) en torno a la protección de los menores en entornos digitales con relación a la protección de sus datos personales

(3) a tener en cuenta al momento de crear o fortalecer las autoridades nacionales de protección de datos en los países iberoamericanos.

A la luz del análisis realizado, se formularán propuestas específicas para orientar el diseño de políticas públicas (regulaciones) en los países iberoamericanos.

Del derecho a la protección de datos en la Carta de los Derechos Fundamentales de la Unión Europea y la autodeterminación informativa en la Corte Interamericana de Derechos Humanos (CIDH).

El 7 de diciembre del año 2000 el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea proclamaron la Carta de los Derechos Fundamentales de la Unión Europea[4] , la cual tiene igual valor jurídico que los tratados internacionales tal y como lo señala el artículo 6 del tratado de la Unión Europea. En el preámbulo de dicho documento se destacó la necesidad de "reforzar la

[4] Cfr. PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, COMISIÓN EUROPEA. 2000. Carta de los derechos fundamentales de la Unión Europea. El texto oficial fue publicado en el Diario Oficial de las Comunidades Europeas C 364/7 del 18 de diciembre de 2000.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos"[5]

En dicha Carta se consagran por separado el derecho al "respeto a la vida privada y familiar"[6] (artículo 7) y el derecho a la "protección de datos de carácter personal"[7] (artículo 8). Con lo anterior se subraya el carácter autónomo e independiente de la protección de datos frente al derecho a la intimidad.

La Carta Europea de Derechos humanos es jurídicamente vinculante a España, Portugal y Andorra . Por ende, el artículo 8 hace parte de la Constitución de dichos países. Dicha Carta, que forma parte de los Tratados UE, está de hecho por encima de la Constitución de los citados países en base al principio de primacía del derecho europeo sobre el derecho local.

La Corte Interamericana de Derechos Humanos (CIDH), por su parte, expresamente reconoció la autodeterminación informativa como un derecho humano autónomo de obligatorio respeto y cumplimiento en el sistema interamericano de derechos humanos. En efecto, en la sentencia Serie C No. 506 de 18 de octubre de 2023 concluyó la CIDH:

> "586. A juicio de la Corte Interamericana, los elementos anteriores dan configuración a **un derecho humano autónomo: el derecho a la autodeterminación informativa**, reconocido en distintos ordenamientos jurídicos de la región743, y que encuentra acogida en el

[5] En el preámbulo también se precisa que la Carta reafirma "los derechos reconocidos especialmente por las tradiciones constitucionales y las obligaciones internacionales comunes de los Estados miembros, el Tratado de la Unión Europea y los Tratados comunitarios, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Comunidad y por el Consejo de Europa, así como por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal Europeo de Derechos Humanos".

[6] "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones" (Artículo 7 de la Carta de los derechos fundamentales de la Unión Europea)

[7] "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la
persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente" (Artículo 8 de la Carta de los derechos fundamentales de la Unión Europea)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

> contenido tutelar de la Convención Americana, en particular a partir de los derechos recogidos en los artículos 11 y 13, y, en la dimensión de su protección jurisdiccional, en el derecho que garantiza el artículo 25." [8]
> (…)
>
> "588. En definitiva, **se trata de un derecho autónomo que sirve, a su vez, de garantía de otros derechos**, como los concernientes a la privacidad, a la protección de la honra, a la salvaguarda de la reputación y, en general, a la dignidad de la persona. Es preciso acotar que el derecho alcanza, con las limitaciones aplicables (infra párrs. 601 a 608), **a cualquier dato de carácter personal en poder de todo órgano público, y opera igualmente respecto de registros o bases de datos a cargo de particulares**, cuestiones sobre las que no se ahonda en razón del objeto de este proceso internacional" [9] (Destacamos)

Se trata de un fallo icónico de enorme relevancia en el sistema interamericano de derechos humanos porque, entre otra, impone deberes a los Estados y abre las puertas para que el mismo se garantizado por tribunales de justicia internacionales.

Adoptar mecanismos para garantizar en la práctica (no en el papel o en la teoría) es, precisamente, uno de los deberes que deben cumplir los Estados tal y como se deriva de lo siguiente que enfatiza la CIDH:

> 599. En todo caso, la Corte Interamericana reitera que **la efectividad del derecho a la autodeterminación informativa exige que los Estados prevean mecanismos o procedimientos adecuados, ágiles, gratuitos y eficaces para dar trámite y atender, por parte de la misma autoridad que administra los datos o por otra institución competente en materia de protección de datos personales o de supervisión** (supra párr. 582)755, (…) **Esta exigencia, derivada del deber que establece el artículo 2 de la Convención Americana**, en cuanto abarca la expedición de normas y el desarrollo de prácticas conducentes a la observancia de los derechos humanos757, incluidos procedimientos administrativos

[8] Cfr. Corte Interamericana de Derechos Humanos Sentencia de 18 de octubre de 2023. Serie C No. 506. El texto oficial de la sentencia puede consultarse en: https://jurisprudencia.corteidh.or.cr/vid/953775991
[9] Cfr. Corte Interamericana de Derechos Humanos Sentencia de 18 de octubre de 2023. Serie C No. 506. El texto oficial de la sentencia puede consultarse en: https://jurisprudencia.corteidh.or.cr/vid/953775991

apropiados, constituye una garantía esencial para hacer valer y ejercer el derecho." [10] (Destacamos)

Necesidad de modernizar las regulaciones para garantizar el debido tratamiento de los datos personales y los derechos humanos en una sociedad digital

A finales de diciembre de 2022 la Organización para la Cooperación y el Desarrollo Económico (OCDE) emitió la Declaración sobre un futuro digital fiable, sostenible[11] en la cual se resalta, entre otros temas, "las conclusiones del Proyecto horizontal de la OCDE sobre gobernanza de datos para el crecimiento y el bienestar (fase III de Going Digital), que reconocen la importancia de los datos como motor de la economía mundial,(..)."

Dicha organización se comprometió a trabajar para, entre otras acciones: a) "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." b) "Garantizar el bienestar de los consumidores capacitándolos para tomar decisiones informadas en el entorno digital y protegiéndolos de las prácticas comerciales engañosas, manipuladoras, fraudulentas, ilícitas y desleales, así como de los bienes y servicios inseguros".[12]

[10] Cfr. Corte Interamericana de Derechos Humanos Sentencia de 18 de octubre de 2023. Serie C No. 506. El texto oficial de la sentencia puede consultarse en: https://jurisprudencia.corteidh.or.cr/vid/953775991

[11] Cfr. OCDE (2022) Declaration on a Trusted, Sustainable and Inclusive Digital Future. La declaración fue fruto de la reunión que se realizó en la Isla Gran Canaria (España) el 14-15 diciembre de 2022. El texto oficial puede consultarse en:

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488

[12] Ídem

El 23 de enero de 2023, el Parlamento Europeo, el Consejo y la Comisión, por su parte, aprobaron la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital[13]. Allí, en el CAPÍTULO III -titulado Libertad de elección- y bajo el subtítulo de "Un entorno digital justo" se comprometieron , entre otros puntos, a lo siguiente: " a) 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; (…)".

Propuesta de Global Privacy Assembly -GPA- (2023)

La Global Privacy Assembly (GPA) adoptó en octubre de 2023 la resolución "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide"[14] mediante la cual se insiste en una idea de hace décadas: contar con estándares globales con respecto a la protección de datos y la privacidad. Para ello, promovió en la declaración algunos principios, derechos y otros elementos como importantes para lograr altos estándares de protección de los citados derechos. En dicho, la GPA resolvió lo siguiente.[15]

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

[14] Cfr. Global Privacy Assembly (GPA). 45th Closed Session of the Global Privacy Assembly. October 2023. Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. En: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

[15] Lo anterior es parte de una traducción libre del autor del siguiente texto oficial en inglés: "The 45th Global Privacy Assembly therefore resolves to:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Abogar por, promulgar y promover los principios, derechos y otros elementos establecidos en esa resolución, para garantizar que puedan implementarse y aplicarse efectivamente en todos los contextos, particularmente en el procesamiento de datos con tecnologías e innovaciones nuevas y emergentes; y
- Solicitar a los legisladores y formuladores de políticas que consulten a las autoridades de protección de datos y privacidad como asesores expertos confiables al promulgar y modificar leyes de protección de datos, privacidad y leyes relacionadas.

En ese documento, GPA enfatizó la "importancia de brindar protección de datos personales a través de fronteras con una variedad de mecanismos de transferencia, como adecuación, cláusulas modelo, certificaciones y acuerdos administrativos, para garantizar que la protección de los datos "viaje" con dicha información cuando la misma circula a través de las fronteras" y 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".[16]

• Advocate for, promulgate and promote the principles, rights and other elements set out in this resolution, to ensure they can be effectively implemented and applied in all contexts, particularly in the processing of data with new and emerging technologies and innovations; and

• Call on law and policy makers to consult data protection and privacy authorities as trusted expert advisers when enacting and amending data protection, privacy and related laws"

Tomado de: Global Privacy Assembly (GPA). 45th Closed Session of the Global Privacy Assembly. October 2023. Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. Pág 9. En:
https://globalprivacyassembly.org/document-archive/adopted-resolutions/

[16] Lo anterior es parte de una traducción libre del autor del siguiente texto oficial en inglés:

"13. International transfers of personal data.

We emphasize the importance of providing for the protection of personal data across borders with a range of transfer mechanisms, such as adequacy, model clauses, certifications and administrative arrangements, to ensure that protection travels with the data. We note the benefits of building on

Con el apoyo de:
Con el apoyo de:
Cooperación Española

La transferencia de información entre países con diferentes culturas jurídicas es una realidad que tiende a continuar creciendo a medida que se incrementan las relaciones sociales y económicas junto con el aumento de usuarios de internet y la inmersión masiva de las TIC en el mundo[17]. Vivimos en una sociedad globalizada e interconectada tecnológicamente en donde internet ha facilitado significativamente las posibilidades de intercambio de información.

Los aspectos jurídicos y económicos son dos dimensiones o facetas de la globalización que han sido impactadas por el uso de las TIC (tecnologías de información y comunicación) y la necesidad del tratamiento de datos personales.

Los procesos de integración económica exponen la necesidad de exportar e importar[18] datos personales entre las empresas privadas, las personas o las autoridades de los diferentes países. De hecho, se ha reconocido que estos procesos han aumentado significativamente los flujos transfronterizos de datos[19] y que fue necesario expedir normas sobre el tratamiento de estos para que se conciliara la protección de la privacidad y la transferencia internacional de los mismos.

---

commonalities, complementarities and elements of convergence in order to foster future interoperability between existing regulatory approaches and mechanisms enabling safe, trustworthy cross border data flows". Tomado de: Global Privacy Assembly (GPA). 45th Closed Session of the Global Privacy Assembly October 2023 Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. En: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

[17] En 1980 la OCDE reconocía que la circulación de datos "se ha incrementado en gran medida en años recientes y que van a aumentarse aún más con la introducción generalizada de nuevas tecnologías de informática y de comunicaciones" (Parte tomada del prólogo del siguiente documento: OCDE. 1980. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales).

[18] En este sentido señala la doctrina que la globalización de las actividades económicas ha intensificado los procesos transfronterizos de intercambio y circulación de información. [DE TERWANGNE, op. cit., p. 17.].

[19] Cfr. Numeral 4 de los considerandos de la Directiva 95/46/CE.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Propuesta de actualización de la ONU (2024)

La ONU, por su parte, mediante el Informe A/79/173 del 17 de julio de 2024 propuso actualizar la resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, titulada "Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales". [20] Allí se reconoce que la citada resolución fue expedida en 1990 para dar respuestas a las realidades socio tecnológicas de esa época, pero que luego de más de cuatro décadas ha cambiado el mundo debido a la información masi a de las tecnologías. A título de ejemplo, se destacan los siguientes:

- "El surgimiento y popularización de Internet revolucionó la forma en que compartimos y accedemos a la información de todas partes del mundo.
- "Los Teléfonos inteligentes se han convertido en dispositivos esenciales para la comunicación, la productividad, 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 almacenar y acceder a datos y aplicaciones en línea de todo el mundo y desde cualquier parte del mundo.
- "El Big Data ha permitido el análisis sofisticado y la toma de decisiones basadas en el procesamiento de grandes cantidades de datos.

[20] El texto de la propuesta contenida en el informe A/79/173 del 17 de julio de 2024 fue presentado por Ana Brian, Relatora Especial de la ONU sobre el derecho a la privacidad, puede consultarse en: https://www.ohchr.org/es/documents/thematic-reports/a79173-report-special-rapporteur-right-privacy-ana-brian-nougreres . El autor de este estudio fue parte del equipo que colaboró en la redacción del informe y de la propuesta.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- "La Inteligencia Artificial está generando enormes expectativas y cambios a partir de algoritmos avanzados e información.
- "El Internet de las cosas (IoT) permite interconectar dispositivos físicos a través de Internet y compartir información para automatizar y controlar remotamente diversos sistemas.
- "La Realidad Virtual y Realidad Aumentada han permitido crear nuevas experiencias digitales, desde juegos hasta aplicaciones de formación y simulaciones.
- "Los Vehículos autónomos que se nutren de los avances en la inteligencia artificial y de los sensores para que los carros pueden operar de manera autónoma, transformando la industria del transporte y la forma de movilización de las personas.
- "Las neurotecnologías permiten el conocimiento minucioso del cerebro y la información neuronal de las personas (datos super sensibles)." [21]

Dado lo anterior, para la ONU "es necesario actualizar esos principios e instituciones para ajustarlos a las realidades de la realidad socio tecnológica del siglo XXI. Pero, adicionalmente, las tecnologías permiten que desde cualquier parte del mundo se recolecten datos de personas domiciliadas o residentes en otros países. Este fenómeno denominado "recolección internacional de datos" [22] está ausente en el texto de la resolución en comento. Y, por ser la forma mediante la cual más se recolectan datos de personas de todas partes del mundo, debería incorporarse en los documentos internacionales." [23]

[21] Cfr. ONU, informe A/79/173 del 17 de julio de 2024

[22] Cfr. Remolina Angarita, Nelson (2015) *Recolección internacional de datos: un reto del mundo postinternet*." BOE – Boletín Oficial del Estado. Madrid, España, abril de 2015. ISBN 978-84-340-2196-9.

[23] Cfr. ONU, informe A/79/173 del 17 de julio de 2024

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Para la elaboración de la propuesta , de una parte, se realizaron algunas adiciones y actualizaciones respecto de los temas existentes de la resolución 45/95 y, de otra parte, se incluyeron nuevos temas, a saber:

- Principio de confidencialidad;
- Protección reforzada a datos sensibles;
- Principio de transparencia;
- Principio de explicabilidad;
- Principio de responsabilidad demostrada o proactiva (accountability);
- Evaluaciones de impacto de tratamiento de datos;
- Privacidad desde el diseño y por defecto, y
- Recolección internacional de datos

Se adjunta a este estudio el texto de la propuesta de actualización para que el lector pueda conocer los detalles y alcance de la misma.

Propuesta de una Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales (2024)

A finales de 2024 fue dada a conocer una propuesta de una Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales, escrita por Luca

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Belli[24] (Brasil), Ana Brian[25] (Uruguay), Jonathan Mendoza[26](México), Pablo Palazzi[27] (Argentina) y Nelson Remolina[28] (Colombia) y publicada en el siguiente libro: Transferencia internacional de dados pessoais na América Latina. Rumo a harmonizacao de normas[29].

---

[24] Luca Belli. Profesor de Gobernanza y Regulación Digital en la Escuela de Derecho de la Fundação Getulio Vargas (FGV), Rio de Janeiro, donde dirige el Centro de Tecnología y Sociedad (CTS-FGV) y el proyecto CyberBRICS.

[25] Ana Brian Nougrères Relatora especial de las Naciones Unidas en materia de Privacidad por el Consejo de Derechos Humanos de las Naciones Unidas. Profesora de la Facultad de Derecho de la Universidad de la República de Uruguay.

[26] Jonathan Mendoza Iserte. Ex secretario de Protección de Datos Personales en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de México.

[27] Pablo Andrés Palazzi. Profesor de Derecho en la Universidad de San Andrés (UDESA). Profesor visitante en la Fundación Getulio Vargas (RJ, Brasil) y en la Fordham Law School (NYC, USA). Director académico del Centro de Tecnología y Sociedad (CETyS) de la Universidad de San Andrés.

[28] Nelson Remolina Angarita. Profesor y Director de la Maestría en derecho, tecnología y sociedad digital de la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia): https://derecho.uniandes.edu.co/programas/posgrados/maestria-en-derecho-tecnologia-y-sociedad-digital/ Director del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática (GECTI) (http://gecti.uniandes.edu.co/) de la Facultad de Derecho de la Universidad de los Andes. Fundador (2008) y director del Observatorio Ciro Angarita Barón sobre la Protección de Datos Personales en Colombia (http://habeasdatacolombia.uniandes.edu.co/).

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Como punto de partida, se pone de presente que las tecnologías digitales ha transformado la forma en que se recopilan, procesan y transfieren datos personales a través de las fronteras y presenta oportunidades y desafíos para individuos, empresas, investigadores e investigadoras y gobiernos de todo el mundo. Se plantea que Latinoamérica se encuentra en una encrucijada generada por, entre otras, las complejidades de las transferencias de datos personales en medio de una rápida innovación tecnológica y una interconexión global. Adicionalmente, "la falta de regulación del fenómeno de la recopilación internacional de datos personales en América Latina[30] crea un vacío muy grande en la región, sobre todo porque muchas de las normas vigentes no tienen aplicación extraterritorial, como sí la tienen el régimen de la Unión Europea y las leyes más modernas" [31]

La versión preliminar de la propuesta fue presentada en la conferencia CPDP LatAm 2023 y 2024 , en Río de Janeiro, Brasil, con el fin de recibir comentarios de quienes asistieron al evento.[32] La versión corregida con comentarios fue publicada en el tomo 4 de la obra colectiva *Protección de datos*

[29] Cfr. Belli, Luca; Brian, Ana; Mendoza, Jonatha; Palazzi, Pablo y Remolina, Nelson. (2024) Transferencia internacional de dados pessoais na América Latina. Rumo a harmonizacao de normas. Lumen Juris editora y Fundación Getulio Vargas. Rio de Janeiro, Brasil. ISBN: 978-85-519-3246-9. El texto está disponible en: https://repositorio.fgv.br/items/98aaa2e4-7279-4649-8dae-836ca8a65bae

[30] REMOLINA, Nelson. *Recolección internacional de datos personales: un reto del mundo post-internet.* Edición Boletín Oficial del Estado, pp 245. 2015. (Premio Protección de Datos Personales de Investigación 2014 Iberoamérica).

[31] Cfr. Belli, Luca; Brian, Ana; Mendoza, Jonatha; Palazzi, Pablo y Remolina, Nelson. (2024) Transferencia internacional de dados pessoais na América Latina. Rumo a harmonizacao de normas. Lumen Juris editora y Fundación Getulio Vargas. Rio de Janeiro, Brasil. ISBN: 978-85-519-3246-9. Pág. 7

[32] Ver Computers Privacy and Data Protection Conference Latin America [https://cpdp.lat/pt-br/programa/].

Con el apoyo de:
Con el apoyo de:
Cooperación Española

personales: doctrina y jurisprudencia (Pablo Palazzi, compilador), Buenos Aires, Argentina, la cual fue premiada por el Future of Privacy Forum con el reconocimiento Privacy Papers for Policymakers Award (2024).

Para lo autores de la propuesta, la posibilidad de que América Latina tenga un tratado internacional sobre protección de datos personales y privacidad es muy importante y ventajosa por lo siguiente:

En primer lugar, la existencia del tratado, una vez aprobado y vigente, permitirá crear un bloque regional de 34 países latinoamericanos con un sistema de protección de datos homogéneo, que tutelara a los habitantes de la región (un total de 660 millones de personas) y permitiera a la región posicionarse frente a otros bloques regionales de una manera diferente a la posición individual que existe ahora. Todo ello con el fin de negociar reconocimientos de adecuación a nivel regional.

En segundo lugar, unifica las reglas a nivel regional para permitir que sean sancionadas por países que no las tienen. Un tratado regional ayudará al crecimiento del derecho a la protección de datos en la región reglamentando las cuestiones internacionales, como las transferencias internacionales de datos, incentivando el libre flujo de datos (tema central para el comercio internacional) o la colaboración directa entre autoridades de protección de datos dentro de un marco reglado (algo que ya se da *de facto* en la región, como lo evidencian los casos de OpenAI).

Adicionalmente, la futura Convención facilita el desarrollo de la protección de datos como un derecho fundamental, ya que el tratado podría encomendar a la Corte Interamericana de Derechos Humanos que actúe como órgano transnacional interpretativo de los derechos contenidos en el acuerdo con efecto vinculante. Esto forzaría a los Estados miembros a realizar un control de convencionalidad de sus respectivas leyes frente al tratado y resultará en una mayor armonización en América Latina.

Finalmente, el tratado podría contemplar la creación de un organismo consultivo y emisor de *soft law*, al estilo del Data Protection Committee del Convenio 108 o de la Comisión Interamericana de

Mujeres, con la obligación de incluir medidas positivas como lo propone la Convención de Belém do Pará.

Estos son algunos de los principales aspecto de la Convención:

En el capítulo I de la propuesta de Convención se consagran los siguientes objetivos de la misma, a saber: "a) Fijar las reglas para garantizar el debido tratamiento de los datos personales y proteger los derechos de las personas titulares de esa información; b) Facilitar el flujo de los datos personales entre los Estados miembros con la finalidad de coadyuvar al crecimiento social y económico y el desarrollo sostenible de la región. c) Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados miembros, las autoridades de control no pertenecientes al Convenio y autoridades y entidades internacionales en la materia."

Adicionalmente, se establecen las principales definiciones junto con los criterios subjetivos y de aplicación territorial de la convención.

En el capítulo II se prevén los principales principios aplicables al tratamiento de datos personales (Dignidad humana, legitimación, consentimiento, licitud, lealtad, buena fe, transparencia, finalidad, minimización, calidad, responsabilidad demostrada, seguridad, confidencialidad, prevención y precaución).

En el capítulo III se enuncia los derechos de los titulares de los datos. Adicionalmente, se fijan reglas especiales para el tratamiento de datos de menores de edad y la información sensibles.

En el capítulo IV se señala que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento deben tomar las medidas necesarias para cumplir con las obligaciones de la Convención y ser capaces de demostrar que el tratamiento de datos bajo su control cumple con la misma. Adicionalmente, se implementa la necesidad de analizar el impacto del tratamiento de datos sobre los derechos y las libertades fundamentales de los titulares de datos, previo al comienzo de dicho tratamiento, y deberán diseñar el tratamiento de datos de manera tal que se prevenga o minimice el riesgo de interferencia con dichos derechos o libertades fundamentales.

El capítulo V consagra las reglas sobre la transferencia y la recolección internacionales de datos personales . En el capítulo VI se fina la naturaleza de las autoridades de control y supervisión. Se exige que las mismas sea autónomas y ajenas a toda influencia externa, ya sea directa o indirecta.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Tampoco podrán solicitar ni admitir orden ni instrucción alguna. Señala la propuesta que la legislación nacional de los Estados miembros que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, auditoría, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de esta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

Se exige en la propuesta que las autoridades de control cuenten con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

El capítulo VII se refiere a los mecanismos interamericanos de protección y hace especial énfasis en la necesidad de contar con una Comisión Interamericana de Protección de Datos Personales como un órgano autónomo y encargado de la promoción y protección de los derechos reconocidos en la Convención en los países miembros. Estará integrada por las autoridades de protección de datos de los países miembros de la Convención.

Se anexa el texto de la citada propuesta de convención interamericana para que el lector pueda conocer los detalles y alcance de la misma.

La protección de datos personales en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales

Las Jefas y Jefes de Estado y de Gobierno de 22 países iberoamericanos[33] aprobaron el 25 de marzo de 2023 la Carta Iberoamericana de Principios y Derechos en Entornos Digitales (CIPDED), la cual "tiene por objeto promover principios comunes para que sean tomados en cuenta por los Estados al momento de adoptar o adecuar las legislaciones nacionales o poner en marcha políticas públicas

[33] Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal, R Dominicana, Uruguay, Venezuela.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

relacionadas con la protección de los derechos y el cumplimiento de los deberes en entornos digitales, así como por las empresas, la sociedad civil y la academia a la hora de desarrollar y aplicar tecnologías, colocando a las personas en el centro de la transformación digital"[34]

Dentro de los diez (10) principios de la CIPDED, se mencionan algunos relacionados con el tratamiento de datos personales y las tecnologías emergentes. Dentro de cada uno de ellos, existen aspectos directamente conexos con el objeto de la presente consultoría que destacaremos a continuación:

Principio1: Centralidad de las personas. Derechos y deberes en entornos digitales.

El principio parte de la regla según la cual "los derechos de todas las personas deben ser garantizados, respetados y protegidos en los entornos digitales" [35]. Por ende, precisa la Carta que "las personas deben verse protegidas en los entornos digitales como sujetos de derechos y deberes" [36].

Dado lo anterior, en la CIPDED se acordó, de una parte, "promover la construcción de una sociedad de la información inclusiva, centrada en las personas y orientada al desarrollo" [37]. Y, de otra parte, "garantizar que el respeto, promoción y protección de los derechos y el cumplimiento de los deberes

[34] Secretaria General Iberoamericana. Cumbre Iberoamericana de Jefas y Jefes de Estado y de Gobierno. Carta Iberoamericana de Principios y Derechos en Entornos Digitales (CIPDED). Adoptada en Santo Domingo, República Dominicana, el 25 de marzo de 2023. En: https://www.segib.org/wp-content/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf . Pág. 8
[35] CIPDED. Pág. 6
[36] CIPDED. Pág. 6
[37] CIPDED. Pág. 6

recogidos en nuestras constituciones y marcos jurídicos se interpretarán, aplicarán y ejercerán en los entornos digitales, teniendo en cuenta sus particularidades" [38]

Principio 3: Privacidad, confianza, seguridad de datos y ciberseguridad.

En torno a ese principio se señala que "deben hacerse esfuerzos relevantes para garantizar que la privacidad de las personas y el procesamiento de sus datos personales estén protegidos en entornos digitales, respetando las legislaciones nacionales en la materia" [39]. Adicionalmente, se pone de presente que "es necesario establecer y actualizar marcos legales que garanticen la privacidad y seguridad en el tratamiento de datos personales para que la transformación digital fortalezca las capacidades de las personas y se convierta en un motor del desarrollo inclusivo a nivel económico, social y cultural al servicio de toda la sociedad" [40]

Dado lo anterior, en la CIPDED se acordó lo que sigue a continuación:

- "Fomentar entornos digitales seguros y confiables, estableciendo medidas para garantizar la protección de la privacidad de las personas y de los datos personales." [41]
- "Continuar y reforzar la cooperación efectiva entre los países del espacio iberoamericano relacionada con la protección de datos personales y privacidad" [42]

[38] CIPDED. Pág. 7
[39] CIPDED. Pág. 12
[40] CIPDED. Pág. 12
[41] CIPDED. Pág. 12
[42] CIPDED. Pág. 13

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Principio 5: Especial atención a niñas, niños y adolescentes

El principio resalta que "las niñas, niños y adolescentes están sujetos a una especial exposición y vulnerabilidad en los entornos digitales" [43], razón por la cual se afirmó que "los derechos fundamentales y en especial el interés superior de niñas, niños y adolescentes deben ser garantizados en los entornos digitales."[44].

En virtud de lo anterior, y relacionado con el tratamiento de datos, se acordó que "es necesario adoptar políticas públicas que tengan por objeto resguardar (…) la privacidad de niñas, niños y adolescentes en los entornos digitales".

Específicamente, en la CIPDED se acordó, entre otras, lo siguiente:

- "Promover políticas activas que tengan por objeto asegurar el respeto a la (…) intimidad y privacidad de niñas, niños y adolescentes en los entornos digitales" [45]
- "Promover que el tratamiento de datos personales de niñas, niños y adolescentes sea el mínimo indispensable para que puedan satisfacer sus necesidades y acceder a los servicios públicos que les correspondan, restringiendo de modo efectivo el uso y procesamiento de datos, sistemas de perfilado y prácticas comerciales destinados a manipular la voluntad de niñas, niños y adolescentes." [46]

[43] CIPDED. Pág. 16
[44] CIPDED. Pág. 17
[45] CIPDED. Pág. 17
[46] CIPDED. Pág. 18

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Principio 9: Un abordaje de las tecnologías emergentes que no renuncie a la centralidad de las personas

El principio reconoce que la "innovación tecnológica y los nuevos desarrollos tecnológicos y científicos, tales como la Inteligencia Artificial, neurotecnologías o computación cuántica, entre otros, suponen retos que deben abordarse garantizando los derechos de las personas." [47]. Por ello, se adquirió el compromiso de, entre otros, lo que sigue a continuación:

- "Abordar conjuntamente las cuestiones asociadas a las tecnologías emergentes, así como su uso seguro, ético y responsable." [48].
- "Promover políticas públicas y marcos normativos que fomenten el desarrollo y uso seguro, ético y responsable de las tecnologías emergentes, en pleno respeto a los propósitos y principios de la Carta de Naciones Unidas y el derecho internacional, incluidos todos los derechos humanos para todas las personas, y con la participación de las múltiples partes, según sus roles y responsabilidades." [49]

Análisis comparativo de documentos internacionales sobre tratamiento de datos personales

El tratamiento de datos personales es una labor cotidiana y global. En todo momento, la información está circulando interna y transfronterizamente. Al mismo tiempo, la misma nutre o alimenta los sistemas de información y bases de datos esenciales para el funcionamiento de internet, la inteligencia artificial, el internet de las otras cosas y muchos otros fenómenos tecnológicos.

[47] CIPDED. Pág. 28
[48] CIPDED. Pág. 29
[49] CIPDED. Pág. 29

Con el apoyo de:
Con el apoyo de:
Cooperación Española

El análisis comprende los siguientes documentos:

- ONU (Organización de las Naciones Unidas), 1990. Resolución 45/95 del 14 de diciembre de 1990 "principios rectores para la reglamentación de los ficheros computadorizados de datos personales"
- APEC (Foro de Cooperación Económica Asia Pacífico) 2004. Marco de Privacidad APEC (APEC Privacy Framework)
- CIAPDP (Autoridades de protección de datos y privacidad), 2009. Estándares internacionales sobre protección de datos personales y privacidad (Resolución de Madrid) -Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad en relación con el Tratamiento de Datos de carácter personal- Madrid, España.
- OCDE (Organización para la Cooperación y el Desarrollo Económico), 2013. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.
- UE (Unión Europea) 2016. 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).
- RIPD (Red Iberoamericana de protección de datos), 2017. Estándares de protección de datos personales para los países Iberoamericanos de la Red Iberoamericana de Protección de Datos[50].
- CdE (Consejo de Europa), 2018. Convenio 108+ de 2018 para la protección de las personas con respecto al tratamiento de datos de carácter personal.
- OEA (Organización de Estados Americanos), 2021. Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones expedidos el 9 de abril de 2021 por el l Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA). Estos principios fueron aprobados por la Asamblea General de la OEA en noviembre de 2021.
- GPA (Global Privacy Assembly), 2023. Resolución "Alcanzando estándares globales de protección de datos: principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo"

[50] Estándares aprobados en el XV Encuentro de la RIPD, que tuvo lugar en Santiago de Chile,, el 22 de junio de 2017.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Es importante tener presente los documentos internacionales por varias razones[51]:

En primer lugar, muestran que la protección de datos personales no es nueva y que su origen no es un capricho del legislador local sino fruto de un movimiento y tendencia internacional para tratar de conciliar las necesidades de los negocios internacionales y el respeto de algunos derechos humanos.

En segundo lugar, nos permiten determinar el origen y alcance de muchos términos, definiciones e instituciones utilizados en las regulaciones locales.

En tercer lugar, nos dan una idea de la evolución o involución regulatoria, según el caso y la opinión del lector, de ciertos aspectos afines al tratamiento de datos personales;

En cuarto lugar, nos ayudan a detectar algunos eventuales vacíos de las regulaciones locales frente al escenario internacional.

En quinto lugar, buena parte de los datos personales de las personas con nacionalidad de los países iberoamericanos son recolectados desde otros países, circulan transfronterizamente o están almacenados en diferentes jurisdicciones extranjeras. Estamos en un mundo global, hiperconectado y cada vez más permeado por diferentes tradiciones jurídicas que debemos conocer y entender para tomar decisiones informadas.

Finalmente, y no menos importante, son herramientas que le permitirán al lector construir sus propias conclusiones sobre el derecho al debido tratamiento de los datos personales.

Se compararán los siguientes aspectos:

[51] Esta parte es una adaptación de las ideas expresadas por el autor en el siguiente libro: Remolina Angarita, Nelson (2013) Tratamiento de datos personales. Aproximación internacional y comentarios a la ley 1581 de 2012". Ed Legis. Bogotá, noviembre de 2013. ISBN: 978-958-767-086-8. Págs 89-90

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Los principios sobre el tratamiento de datos personales
- Los derechos de las personas titulares de los datos personales
- Las medidas proactivas para garantizar el debido tratamiento de la información mencionada
- Las alternativas para realizar transferencias internacionales, y
- Las características que deben cumplir las autoridades de control o de protección de datos.

A partir de lo anterior se contará con información que permite cuantificar el grado de cumplimiento de cada documento internacional sobre los aspectos comparados.

Es importante tener presente lo siguiente[52]:

- Por tener diferente origen es entendible que la denominación y alcance de los temas analizados no sea idéntica en los documentos emitidos por las organizaciones enunciadas anteriormente (ONU, APEC, CIAPDP, OCDE, UE, RIPD, CdE, OEA y GPA). No obstante, los grandes mensajes o fundamentos de cada tema suelen coincidir aunque la redacción y alcance sea diversa no sólo porque provienen de diferentes entidades sino porque su versión original fue escrita en otros idiomas diferentes al castellano (inglés).
- Los documentos internacionales son fruto de una labor de armonización de los aspectos centrales del tratamiento de datos personales. Procuran asegurar unos mínimos en las actividades que impliquen la recolección, almacenamiento y uso de dicha información, estableciendo unos principios sobre la materia e imponiendo, en ciertos casos, criterios de comportamiento razonable.
- Dado su origen extranjero reflejan conceptos, instituciones y finalidades de otras culturas y sistemas jurídicos que, según el país, pueden coincidir o ser consistentes con las tradiciones jurídicas locales. Han sido el modelo o guía de referencia de normas locales y un referente para interpretar o suplir vacíos de las mismas.
- Las expresiones y alcances que le dan los documentos internacionales a ciertos principios e instituciones no necesariamente coinciden con los términos de las regulaciones locales;
- No todos los documentos mencionan los mismos temas. Por ejemplo, la mayoría se refieren al principio de seguridad y a las reglas sobre transferencias internacionales pero no todos definen que es un dato personal, la autorización o el consentimiento.

[52] Esta parte es una adaptación de las ideas expresadas por el autor en el siguiente libro: Remolina Angarita, Nelson (2013) Tratamiento de datos personales. Aproximación internacional y comentarios a la ley 1581 de 2012". Ed Legis. Bogotá, noviembre de 2013. ISBN: 978-958-767-086-8. Pág 90

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- En algunos casos y para ciertas cuestiones los términos utilizados en los documentos internacionales son muy amplios, lo cual dificulta tener certeza objetiva de lo que se quiere o no se quiere.
- Finalmente, todas las organizaciones parten del supuesto de respetar derechos humanos pero la misión principal o razón de ser algunas entidades son el crecimiento económico (APEC[53]), el bienestar económico y social (OECD[54]), lo cual explica porque en ciertos documentos se incluyen o excluyen ciertas cuestiones o se hace énfasis en unas cosas y se dejan de lado otras.
- Los documentos internacionales provienen de lugares (Europa, Norteamérica, Latinoamérica) con diferentes sistemas de tradición jurídica. Así las cosas, su interpretación y alcance deben considerar las diversas culturas jurídicas que están inmersas en cada texto. En otras palabras, los textos establecen reglas generales aplicables al tratamiento de datos personales pero fueron redactados en países con disímiles tradiciones jurídicas, condiciones económicas y políticas. Reflejan algunos conceptos que se encuentran en varios sistemas jurídicos pero no reemplazan dichos sistemas ni borran absolutamente las normas, culturas y tradiciones jurídicas locales.
- Los documentos internacionales procuran armonizar mínimos para el tratamiento global de datos personales, pero no unifican dichas reglas. Pese a lo anterior, recalcamos, no dejan de ser muy importantes y deben tenerse en cuenta.

Los principales resultados son los siguientes:

[53] APEC es el foro económico Asia-Pacífico y su principal objetivo es apoyar el crecimiento económico sostenible y la prosperidad en la región Asia-Pacífico. Procuran defender el comercio y la inversión, promover y acelerar la integración económica regional, fomentar la cooperación económica y técnica, mejorar la seguridad humana, y facilitar un ambiente de negocios favorable y sostenible .(Cfr. http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx . Última consulta: agosto 7 de 2013) Más información sobre APEC en: http://www.apec.org/

[54] La misión de la Organización para la Cooperación y el Desarrollo Económico (OCDE) es promover políticas que mejoren el bienestar económico y el bienestar social de las personas en todo el mundo. La OCDE es un foro en el que los gobiernos pueden trabajar juntos para compartir experiencias y buscar soluciones a problemas comunes e impulsar cambios económicos, sociales y medioambientales. .(Cfr. http://www.oecd.org/about/ . Última consulta: agosto 7 de 2013) Más información sobre la OECD en: http://www.oecd.org/

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Principios sobre el tratamiento de datos personales en documentos internacionales

Los siguientes son los principales principios identificados en los documentos internacionales: Legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad (veracidad), responsabilidad (accountability), seguridad, confidencialidad, temporalidad, prevención del daño y no discriminación.

Del análisis comparativo se destaca lo siguiente:

- En todos los documentos (100%) revisados se incorporan los principios de licitud, finalidad, proporcionalidad y calidad (veracidad).
- En casi todos los documentos (89%) también se incluyen expresamente los principios de legitimación, lealtad, transparencia y responsabilidad (accountability)
- En buena parte de los documentos (67%) también se consagran explícitamente los principios de confidencialidad y temporalidad.
- En pocos documentos (44%) se incluye el principio de no discriminación.
- En muy pocos documentos (22%) se menciona expresamente el principio de prevención del daño.
- Los documentos más recientes mencionan el 100% de los principios, tal y como sucede con GPA (2023). Le siguen con un 92% la RIPD y OEA. Finalmente, con un 85% los documentos de UE (2016) y CdE (2018).

Todo lo anterior se constata en la siguiente tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Principios sobre tratamiento de datos personales que expresamente se incorporan en documentos internacionales														
	Legitimación	Licitud	Lealtad	Transparencia	Finalidad	Proporcionalidad	Calidad	Responsabilidad	Seguridad	Confidencialidad	Temporalidad	Prevención del daño	No discriminación	%
ONU (1990)	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗	✓	62%
APEC (2004)	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	69%
CIAPDP (2009)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	77%
OCDE (2013)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	69%
UE (2016)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	85%
RIPD (2017)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	92%
C 108+ (2018)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	85%
OEA (2021)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	92%
GPA (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
TOTAL	89%	100%	89%	89%	100%	100%	100%	89%	100%	67%	67%	22%	44%	

Tabla 1. Principios sobre tratamiento de datos personales en documentos internacionales

De otra parte, en el informe ONU A/77/196 del 20 de julio de 2022 se realizó un estudio comparativo de siete documentos internacionales para conocer el alcance de los siguientes principios sobre tratamiento de datos personales: legalidad, licitud y legitimidad; consentimiento; transparencia; finalidad; lealtad; proporcionalidad; minimización; calidad; responsabilidad y seguridad. Adicionalmente, se destacaron los elementos comunes de los documentos internacionales respecto de los principios para crear puentes entre los mismos o puntos de contacto que faciliten la armonización en el contexto global.

En el citado informe se concluyó lo siguiente:

> "138. 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.
>
> "139. 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

Con el apoyo de:
Con el apoyo de:
Cooperación Española

base la configuración de algunas de las causales legitimantes establecidas en la normativa que sea de aplicación.

“140. 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.

“141. El principio de transparencia debe observarse independientemente de cuál sea la base jurídica que legitima el tratamiento.

“142. 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.

“143. 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.

“144. 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.

“145. 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.

“146. 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.

“147. 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.

“148. 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.

> "149. 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.
>
> "150. 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."[55]

Adicionalmente, la ONU también presentó un informe 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[56], con miras a verificar ¿qué ha pasado?, ¿qué está pasando? o ¿qué pasará? con los datos de millones de personas de todos los países del mundo que se recolectaron para combatir la pandemia.

Del análisis de 20 países de África, América, Asia, Europa y Oceanía se emitieron algunas conclusiones y se formularon las siguientes recomendaciones:

[55] Cfr. ONU. Informe A/77/196 del 20 de julio de 2022: Principios que informan la privacidad y la protección de datos personales - Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères. En: En: https://www.ohchr.org/es/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data

[56] Cfr. ONU. Informe A/HRC/52/37 del 27 de diciembre de 2022: 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, Ana Brian Nougrères. En: https://www.ohchr.org/es/documents/thematic-reports/ahrc5237-implementation-principles-purpose-limitation-deletion-data-and

Con el apoyo de:
Con el apoyo de:
Cooperación Española

"27. (…) 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.

"28. (…) 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.

"29. (…)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.

"30. 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.

"31. (…) 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.

"32. (…)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

Con el apoyo de:
Con el apoyo de:
Cooperación Española

términos y condiciones de actividades que implican la recolección, el uso, la circulación o cualquier otra actividad en la que se traten datos personales" [57]

Derechos de las personas respecto del tratamiento de datos personales en documentos internacionales

Los siguientes son los principales derechos de las personas en los documentos internacionales: Acceso, rectificación, cancelación, oposición, portabilidad, no ser objeto de decisiones individuales automatizadas e indemnización.

Del análisis comparativo sobresale lo que sigue a continuación:

- En casi todos los documentos (89%) se incluyen expresamente los derechos de acceso y rectificación.
- En buena parte de los documentos (67%) también se consagran explícitamente los derechos de cancelación y oposición.
- En pocos documentos (56%) se incluye el derecho a no ser objeto de decisiones individuales automatizadas.
- En muy pocos documentos (44%) se mencionan expresamente los derechos de portabilidad e indemnización.
- Los siguientes documentos mencionan el 100% de los derechos: UE (2016), RIPD (2017) y GPA (2023). Le siguen OEA (86%) y CdE (71%).

[57] Cfr. ONU. Informe A/HRC/52/37 del 27 de diciembre de 2022. Pág 7-8

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Lo anterior se pone de presente en la siguiente tabla:

Derechos de la persona titular del dato que expresamente se mencionan en documentos internacionales								
	Acceso	Rectificación	Cancelación	Oposición	Portabilidad	No ser objeto a decisiones individuales	Indemnización	%
ONU (1990)	✗	✗	✗	✗	✗	✗	✗	0%
APEC (2004)	✓	✓	✗	✗	✗	✗	✗	29%
CIAPDP (2009)	✓	✓	✓	✓	✗	✓	✗	71%
OCDE (2013)	✓	✓	✗	✗	✗	✗	✗	29%
UE (2016)	✓	✓	✓	✓	✓	✓	✓	100%
RIPD (2017)	✓	✓	✓	✓	✓	✓	✓	100%
C 108+ (2018)	✓	✓	✓	✓	✗	✓	✗	71%
OEA (2021)	✓	✓	✓	✓	✓	✗	✓	86%
GPA (2023)	✓	✓	✓	✓	✓	✓	✓	100%
TOTAL	89%	89%	67%	67%	44%	56%	44%	

Tabla 2. Derechos de la persona titular del dato en documentos internacionales

De otra parte, en el informe ONU A/HRC/55/46 del 18 de enero de 2024 se realizó un estudio comparativo sobre los mecanismos legales de salvaguarda para la protección de datos personales y la privacidad en la era digital. Igualmente, se examinaron los mecanismos legales de los que

Con el apoyo de:
Con el apoyo de:
Cooperación Española

disponen 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 concierne[58].

Estas son algunas de las conclusiones:

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 con 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 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 luego de la denegatoria del mismo, por parte del responsable del tratamiento, existen aspectos de regulación convergente. Entre las particularidades contenidas en determinadas

[58] Cfr. ONU. Informe A/HRC/55/46 del 18 de enero de 2024: 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. En: https://www.ohchr.org/es/documents/thematic-reports/ahrc5546-legal-safeguards-personal-data-protection-and-privacy-digital

Con el apoyo de:
Con el apoyo de:
Cooperación Española

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 datos personales que haya sufrido daños y perjuicios como consecuencia de una infracción en la legislación sobre protección de datos y privacidad" [59].

Dentro de las principales recomendaciones, la Relatora Especial 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;

[59] Cfr. ONU. Informe A/HRC/55/46 del 18 de enero de 2024. Págs. 25-26

Con el apoyo de:
Con el apoyo de:
Cooperación Española

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." [60].

Medidas proactivas para el debido tratamiento de datos personales en documentos internacionales

Las siguientes son las principales medidas proactivas para garantizar el debido tratamiento de los datos personales: privacidad desde el diseño, privacidad por defecto, nombramiento de un oficial de cumplimiento o delegado de datos, mecanismos de autorregulación y evaluaciones de impacto de privacidad o de tratamiento de datos personales.

Lo siguiente se destaca del análisis comparativo:

- En casi todos los documentos (78%) se incluyen expresamente los mecanismos de autorregulación y evaluaciones de impacto de privacidad o de tratamiento de datos personales.
- En buena parte de los documentos (67%) también se consagra la privacidad desde el diseño.
- En muy pocos documentos (44%) se mencionan expresamente las medidas de privacidad por defecto y la figura del oficial de protección de datos.
- Los siguientes documentos mencionan el 100% de las medidas proactivas: UE

[60] Cfr. ONU. Informe A/HRC/55/46 del 18 de enero de 2024. Pág. 26

(2016), RIPD (2017) y GPA (2023). Le siguen OEA (80%), CdE y APEC (60%).

Esto se constata en esta tabla:

Medidas proactivas para el tratamiento de datos personales que expresamente se mencionan en documentos internacionales						
	Privacidad por diseño	Privacidad por defecto	Oficial de protección de datos	Mecanismos de autorregulación	Evaluación de impacto	%
ONU (1990)	✗	✗	✗	✗	✗	0%
APEC (2004)	✓	✗	✗	✓	✓	60%
CIAPDP (2009)	✗	✗	✗	✓	✓	40%
OCDE (2013)	✗	✗	✗	✓	✗	20%
UE (2016)	✓	✓	✓	✓	✓	100%
RIPD (2017)	✓	✓	✓	✓	✓	100%
C 108+ (2018)	✓	✗	✓	✗	✓	60%
OEA (2021)	✓	✓	✗	✓	✓	80%
GPA (2023)	✓	✓	✓	✓	✓	100%
TOTAL	67%	44%	44%	78%	78%	

Tabla 3. Medidas proactivas para el tratamiento de datos personales en documentos internacionales

Alternativas para realizar transferencias internacionales de datos personales

La exportación y la importación de información personal no pueden convertirse en un escenario reductor del nivel de protección que se le confiere al titular del dato en el país desde donde se

Con el apoyo de:
Con el apoyo de:
Cooperación Española

exportan datos personales. Frente a la preocupación internacional de los Estados cuando los datos de sus ciudadanos circulan a través de sus fronteras, se ha establecido como regla general que no se deben enviar datos a países que no garanticen un nivel adecuado de protección.

Como es sabido, las regulaciones sobre transferencia internacional de datos o "flujo transfronterizo de datos" procuran garantizar que el nivel de protección de los datos personales de los ciudadanos de un país no disminuya o desaparezca cuando estos deben ser exportados o transferidos a otro u otros países.

Las siguientes son las principales alternativas para realizar transferencias internacionales de datos personales: Nivel adecuado de protección de datos, cláusulas contractuales, normas corporativas vinculantes, mecanismos de certificación, autorización de la autoridad de control o del titular del dato y tratados internacionales.

Lo siguiente se destaca del análisis comparativo:

- En casi todos los documentos (89%) se incluye expresamente la figura del nivel adecuado de protección que debe tener el país destinatario o receptor de los datos.
- En buena parte de los documentos (56%) también se consagras las normas corporativas vinculantes.
- En muy pocos documentos (44%) se mencionan expresamente las cláusulas contractuales y la autorización de control. Le siguen con un 33% las siguientes alternativas: mecanismos de certificación, autorización del titular del dato y tratados internacionales.
- Los siguientes documentos mencionan el 100% de las alternativas: UE (2016) y RIPD (2017). Le siguen CdE (71%), GPA y CIAPDP (43%).

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Lo anterior se ilustra en esta tabla:

Alternativas para realizar transferencias internacionales de datos personales que expresamente se incorporan en documentos internacionales								
	Nivel adecuado de protección de datos	Cláusulas contractuales	Normas Corporativas vinculantes	Mecanismos de certificación	Autorización de autoridad de control	Autorización de titular del dato	Tratados internacionales	%
ONU (1990)	✓	✗	✗	✗	✗	✗	✗	14%
APEC (2004)	✓	✗	✗	✗	✓	✗	✗	29%
CIAPDP (2009)	✓	✓	✓	✗	✗	✗	✗	43%
OCDE (2013)	✗	✗	✓	✗	✗	✗	✗	14%
UE (2016)	✓	✓	✓	✓	✓	✓	✓	100%
RIPD (2017)	✓	✓	✓	✓	✓	✓	✓	100%
C 108+ (2018)	✓	✗	✓	✗	✓	✓	✓	71%
OEA (2021)	✓	✗	✗	✗	✗	✗	✗	14%
GPA (2023)	✓	✓	✗	✓	✗	✗	✗	43%
TOTAL	89%	44%	56%	33%	44%	33%	33%	

Tabla 4. Alternativas para realizar transferencias internacionales de datos personales según documentos internacionales

Características que deben tener las autoridades de protección de datos personales

Los principales requisitos que deben tener las autoridades de control o de protección de datos son: autonomía, imparcialidad, independencia, ser ajenas a toda influencia externa, tener poderes o facultades de investigación y sanción, contar con suficientes recursos humanos y materiales para cumplir sus funciones, así como contar con competencia técnica en su equipo humano.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Del análisis comparativo sobresale lo que sigue a continuación:

- En casi todos los documentos (89%) se incluye expresamente la independencia.
- En buena parte de los documentos (78%) también se consagras la necesidad de que las autoridades tengan poderes o facultades de investigación y sanción. Le sigue en un 67% la importancia de que el equipo humano de autoridad cuente con competencia técnica (conocimiento regulación de tratamiento de datos personales). Adicionalmente, un 56% exige que las mismas sean imparciales y que cuenten con suficientes recursos humanos y materiales para cumplir sus funciones.
- En muy pocos documentos se menciona expresamente la autonomía (44%) y que la autoridad sea ajena a toda influencia (33%).
- Los siguientes documentos mencionan el 100% todas las características: UE (2016) y RIPD (2017). Le siguen CdE y GPA (71%).

Lo anterior se puede verificar en esta tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Requisitos que expresamente exigen documentos internacionales sobre las autoridades de control o protección de datos personales								
	Autonomía	Imparcialidad	Independencia	Ajena a toda influencia externa	Poderes de investigación, sanción y otros	Recursos humanos y materiales para cumplir funciones	Competencia técnica	%
ONU (1990)	✗	✓	✓	✗	✗	✗	✓	43%
APEC (2004)	✗	✗	✗	✗	✗	✗	✗	0%
CIAPDP (2009)	✗	✓	✓	✗	✓	✗	✓	57%
OCDE (2013)	✗	✗	✓	✓	✓	✗	✓	57%
UE (2016)	✓	✓	✓	✓	✓	✓	✓	100%
RIPD (2017)	✓	✓	✓	✓	✓	✓	✓	100%
C 108+ (2018)	✓	✓	✓	✗	✓	✓	✗	71%
OEA (2021)	✗	✗	✓	✗	✓	✓	✗	43%
GPA (2023)	✓	✗	✓	✗	✓	✓	✓	71%
TOTAL	44%	56%	89%	33%	78%	56%	67%	

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

Los principales resultados son los siguientes:

En términos generales, los datos comparativos muestran que los estándares de la RIPD: (i) cubren un alto porcentaje de principios de protección de datos[61], pero no aborda en detalle algunos relevantes como la prevención del daño; (ii) coinciden con los documentos más actuales en

[61] Como los siguientes principios: Legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad (veracidad), responsabilidad (accountability), seguridad, confidencialidad, temporalidad, y no discriminación

Con el apoyo de:
Con el apoyo de:
Cooperación Española

términos de derechos[62] de los titulares y medidas proactivas[63]; (iii) son robustos en cuanto a alternativas para transferencias internacionales[64] y (iv) son completos frente a los requerimientos que deben reunir las autoridades de protección de datos[65].

Pese a que los estándares de la RIPD contienen temas claves para el debido tratamiento de datos, aún están ausentes en los mismos aspectos relacionados principalmente con las neurotecnologías y la inteligencia artificial. Adicionalmente, su contenido se puede fortalecer para mejorar el nivel de protección de los datos de los menores de edad. Esto, convertiría a los estándares de la RIPD en un referente moderno para la protección de datos frente a tecnologías emergentes.

La actualización de los estándares de la RIPD no es simplemente una cuestión de mantenernos al día con los desarrollos internacionales; es una cuestión de asegurar que nuestros ciudadanos, en particular los más jóvenes y vulnerables, estén protegidos de manera efectiva en un mundo digital cada vez más complejo. Por eso, es necesario apoyar la actualización de los estándares iberoamericanos como una inversión en la protección de los derechos fundamentales de nuestros ciudadanos y en el fortalecimiento de nuestras instituciones para enfrentar los desafíos del futuro.

---

[62] Como los siguientes derechos: Acceso, rectificación, cancelación, oposición, portabilidad, no ser objeto de decisiones individuales automatizadas e indemnización

[63] Las principales medidas proactivas para garantizar el debido tratamiento de los datos personales: privacidad desde el diseño, privacidad por defecto, nombramiento de un oficial de cumplimiento o delegado de datos, mecanismos de autorregulación y evaluaciones de impacto de privacidad o de tratamiento de datos personales

[64] Las principales alternativas para realizar transferencias internacionales de datos personales: Nivel adecuado de protección de datos, cláusulas contractuales, normas corporativas vinculantes, mecanismos de certificación, autorización de la autoridad de control o del titular del dato y tratados internacionales

[65] Los principales requisitos que deben tener las autoridades de control o de protección de datos son: autonomía, imparcialidad, independencia, ser ajenas a toda influencia externa, tener poderes o facultades de investigación y sanción, contar con suficientes recursos humanos y materiales para cumplir sus funciones, así como contar con competencia técnica en su equipo humano.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

La actualización es un paso fundamental para garantizar que nuestras normativas sigan siendo relevantes y eficaces en un panorama tecnológico que no deja de evolucionar.

Algunos aspectos sobre protección de datos personales en las constituciones de los países miembros de la SEGIB

La mayoría de los países Iberoamericanos han modificado sus Constituciones para incorporar aspectos relacionados con los datos personales, el tratamiento de esa clase de información y la protección de los mismos. Este reconocimiento constitucional subraya la intención de asegurar que el tratamiento de los datos personales se maneje con el debido cuidado y respeto, garantizando así los derechos de las personas en toda la región.

Ese estatus constitucional del citado tema, o la "constitucionalización" del mismo, pone de presente el deseo para que en la región se garantice a las personas un debido tratamiento de sus datos personales y, al mismo tiempo refleja un compromiso al más alto nivel por garantizar que se respete y proteja la información personal de los ciudadanos.

Son disímiles las formas como en los diferentes países se ha constitucionalizado el tema en cuestión. Algunos lo tratan bajo el rótulo del habeas data y la acción de amparo, mientras otros lo mencionan en el contexto del derecho de acceso a la información frente a las entidades públicas. Unos realizan una aproximación limitada el tema y otros son más prolijos en la forma de abordar la información sobre las personas y su protección constitucional.

Según datos obtenidos de nuestro análisis, el **82%** de los países incorporan en su Constitución disposiciones explícitas referentes a aspectos relacionados con la protección de datos personales. Particularmente, hacen referencia a, entre otros, los datos personales, la información personal o los

Con el apoyo de:
Con el apoyo de:
Cooperación Española

datos, lo cual pone de presente la importancia de esta categoría de información jurídica de relevancia constitucional.

De otra parte, el **45%** de las constituciones incorpora el derecho a la protección de datos o de información personal. Y un **41%** de las mismas hace alusión a la acción o garantía de habeas data, la acción de amparo o de protección de privacidad.

Este fenómeno constitucional sobre protección de datos en Iberoamérica se ha gestado desde mediados de la década de los ochenta en donde Guatemala (1985), Nicaragua (1987) y Brasil (1988) fueron los primeros países que incorporaron en sus constituciones artículos que mencionan cuestiones relacionadas con la protección de datos personales. Posteriormente, seis países (Colombia, Paraguay, Perú, Argentina, Ecuador y Venezuela) hicieron lo propio durante la década de los años noventa y cinco (Bolivia, Panamá, Honduras, México y República Dominicana) incluyeron en sus reformas constitucionales a partir del año 2000 el tema en comento, siendo los más recientes México (2009 y 2008) y República Dominicana (2010). Mas recientemente Chile (2018), Cuba (2019) y Brasil (2022) reformaron sus constituciones para incluir aspectos sobre tratamiento de datos personales.

Todo lo anterior se sustenta en la información resumida en la siguiente tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Protección de datos / habeas data / tratamiento de datos en las constitucionales iberoamericanos				
	Menciona los datos personales, la información personal o el dato	Incorpora el derecho a la protección de datos o de información personal	Se refiere a la acción o garantía de habeas data /acción de amparo o de protección de privacidad	%
AND	✓	✓	✗	67%
ARG	✓	✗	✓	67%
BOL	✓	✗	✓	67%
BRA	✓	✓	✓	100%
COL	✓	✗	✗	33%
CRI	✗	✗	✗	0%
CUB	✓	✗	✗	33%
CHL	✓	✓	✗	67%
DOM	✓	✓	✗	67%
ECU	✓	✓	✓	100%
SLV	✗	✗	✗	0%
ESP	✓	✓	✗	67%
GTM	✗	✗	✗	0%
HND	✓	✗	✓	67%
MEX	✓	✓	✗	67%
NIC	✓	✗	✗	33%
PAN	✓	✓	✓	100%
PRY	✓	✗	✓	67%
PER	✓	✗	✓	67%
PRT	✓	✓	✗	67%
URY	✗	✗	✗	0%
VEN	✓	✓	✓	100%
TOTAL	82%	45%	41%	

Tabla . Algunos aspectos sobre protección de datos personales mencionados expresamente en las constituciones de los países miembros de la SEGIB

Con el apoyo de:
Con el apoyo de:
Cooperación Española

En adición a los textos constitucionales, la mayoría de los países iberoamericanos con regulaciones generales y especiales de datos. En el siguiente mapa ilustramos las principales disposiciones constitucionales y las leyes que tendremos en cuenta para efectos del presente estudio. Esto lo ilustramos en el siguiente mapa y la referencia a las principales normas las incluimos en el anexo 2.

Mapa 1. Disposiciones constitucionales y normas generales sobre tratamiento de datos personales en los países miembros de la SIGEB

Con el apoyo de:
Con el apoyo de:
Cooperación Española

A continuación, realizaremos un análisis comparativo de las normas generales de tratamiento de datos de los países miembros de la SIGEB.

Análisis comparativo de las regulaciones sobre tratamiento de datos personales en los países miembros de la SEGIB

En las siguientes líneas se efectuará un análisis comparativo de las regulaciones generales sobre tratamiento de datos personales de los siguientes países miembros de la SEGIB: Andorra, Argentina, Bolivia, Brasil, Colombia, Costa Rica, Cuba, Chile, Ecuador, El Salvador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal, República Dominicana, Uruguay y Venezuela.

Se compararon los siguientes aspectos:

- Los principios sobre el tratamiento de datos personales
- Los derechos de las personas titulares de los datos personales
- Las medidas proactivas para garantizar el debido tratamiento de la información mencionada
- Las alternativas para realizar transferencias internacionales desde los países miembros de la SEGIB a otros países, y
- Las características que deben cumplir las autoridades de control o de protección de datos.

A partir de una revisión de las normas generales se generarán información cuantitativa que permitirá cuantificar el grado de cumplimiento de cada país respecto de los aspectos comparados. Esto le permitirá a cada país reflexionar sobre la necesidad de crear o mejorar su regulación de datos personales.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Es importante tener presente lo siguiente:

- Los resultados son producto de la comparación de las normas generales sobre tratamiento de datos personales (en adelante NGTDP). No tendrán en cuenta las normas sectoriales como, entre otras, las relacionadas a los burós de crédito, censos de población o historias clínicas
- De los 22 países analizados, 4 no tienen normas generales sobre tratamiento de datos personales (Bolivia, Guatemala, Honduras y Venezuela). Es decir que sólo el 81,82% cuenta con NGTDP y un 18,18% carece de dicha regulación.

Principios sobre el tratamiento de datos personales en la regulación de los países miembros de la SEGIB.

Los siguientes son los principales principios identificados en los documentos internacionales: Legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad (veracidad), responsabilidad (accountability), seguridad, y confidencialidad.

Por tener diferente origen es entendible que la denominación y alcance de los principios no sea idéntica en las regulaciones de cada país. No obstante, los grandes mensajes o fundamentos de cada principio suelen coincidir, aunque la redacción y alcance sea diversa.

Del análisis comparativo se destaca lo siguiente:

- En casi todas las regulaciones (82%) se incluyen expresamente los principios de transparencia, finalidad, seguridad y confidencialidad. Le siguen en un 77% los principios de licitud y lealtad.
- En buena parte de las normas (68%) también se consagran explícitamente los principios de legitimación, proporcionalidad, calidad y responsabilidad (accountability).

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- El 50% de los países mencionan el 100% de los principios.

Todo lo anterior, y otros aspectos, se constata en la siguiente tabla:

Principios sobre tratamiento de datos personales en las regulaciones de los países miembros de la SEGIB											
	Legitimación	Licitud	Lealtad	Transparencia	Finalidad	Proporcionalidad	Calidad	Responsabilidad	Seguridad	Confidencialidad	%
AND	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
ARG	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	80%
BOL	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
BRA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
COL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
CRI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
CUB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
CHL	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	90%
DOM	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	90%
ECU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
SLV	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	80%
ESP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
GTM	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0%
HND	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0%
MEX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
NIC	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	80%
PAN	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	80%
PRY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
PER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
PRT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
URY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%
VEN	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0%
TOTAL	73%	77%	77%	82%	82%	73%	73%	73%	82%	82%	

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Tabla 6. Principios sobre tratamiento de datos personales en las regulaciones de los países miembros de la SEGIB (31/XII/2024)

Derechos de las personas respecto del tratamiento de datos personales en la regulación de los países miembros de la SEGIB

Los siguientes son los principales derechos de las personas en las regulaciones de los países: Acceso, rectificación, cancelación, oposición, portabilidad, no ser objeto de decisiones individuales automatizadas, limitación del tratamiento e indemnización.

Del análisis comparativo sobresale lo que sigue a continuación:

- En casi todos los documentos (82%) se incluyen expresamente los derechos de acceso, rectificación y cancelación.
- En buena parte de las normas locales (68%) también se consagran explícitamente los derechos de oposición y portabilidad.
- En pocas regulaciones se incluye el derecho a no ser objeto de decisiones individuales automatizadas (59%).
- En muy pocos documentos se mencionan expresamente los derechos de limitación del tratamiento (50%) e indemnización (45%).
- El 31,81% de los países incluyen en sus regulaciones el 100% de los derechos.

Lo anterior se pone de presente en la siguiente tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Derechos de la persona titular del dato en las regulaciones de los países miembros de la SEGIB									
	Acceso	Rectificación	Cancelación	Oposición	Portabilidad	No ser objeto a decisiones individuales automatizadas	Limitación del tratamiento	Indemnización	%
AND	✓	✓	✓	✓	✓	✓	✓	✓	100%
ARG	✓	✓	✓	✗	✗	✗	✗	✗	38%
BOL	✗	✗	✗	✗	✗	✗	✗	✗	0%
BRA	✓	✓	✓	✓	✓	✓	✓	✓	100%
COL	✓	✓	✓	✗	✗	✗	✗	✗	38%
CRI	✓	✓	✓	✓	✗	✓	✓	✓	88%
CUB	✓	✓	✓	✓	✓	✓	✓	✓	100%
CHL	✓	✓	✓	✓	✓	✓	✓	✓	100%
DOM	✓	✓	✓	✓	✓	✓	✗	✓	88%
ECU	✓	✓	✓	✓	✓	✓	✓	✗	88%
SLV	✓	✓	✓	✓	✓	✗	✗	✗	63%
ESP	✓	✓	✓	✓	✓	✓	✓	✓	100%
GTM	✗	✗	✗	✗	✗	✗	✗	✗	0%
HND	✗	✗	✗	✗	✗	✗	✗	✗	0%
MEX	✓	✓	✓	✓	✓	✓	✗	✗	75%
NIC	✓	✓	✓	✓	✓	✗	✗	✗	63%
PAN	✓	✓	✓	✓	✓	✗	✗	✓	75%
PRY	✓	✓	✓	✓	✓	✓	✓	✗	88%
PER	✓	✓	✓	✓	✓	✓	✓	✓	100%
PRT	✓	✓	✓	✓	✓	✓	✓	✓	100%
URY	✓	✓	✓	✗	✓	✓	✓	✗	75%
VEN	✗	✗	✗	✗	✗	✗	✗	✗	0%
TOTAL	82%	82%	82%	68%	68%	59%	50%	45%	

Tabla 7. Derechos de la persona titular del dato en la regulación

de los países miembros de la SEGIB (31/XII/2024)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Medidas proactivas para el debido tratamiento de datos personales en la regulación de los países miembros de la SEGIB

Las siguientes son las principales medidas proactivas para garantizar el debido tratamiento de los datos personales: privacidad desde el diseño, privacidad por defecto, nombramiento de un oficial de cumplimiento o delegado de datos, mecanismos de autorregulación y evaluaciones de impacto de privacidad o de tratamiento de datos personales.

Lo siguiente se destaca del análisis comparativo:

- En muy pocas regulaciones (50%) se mencionan expresamente los mecanismos de autorregulación. Le siguen la figura del oficial de protección de datos y las evaluaciones de impacto de privacidad o de protección de datos (45%)
- Casi ninguna regulación prevé la privacidad desde el diseño y por defecto (27%).
- Solo el 22,7% de los países incluyen en su regulación del 100% de las medidas proactivas.

Esto se constata en esta tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Medidas proactivas en las regulaciones de los países miembros de la SEGIB

	Privacidad por diseño	Privacidad por defecto	Oficial de protección de datos	Mecanismos de autorregulación	Evaluación de impacto	%
AND	✓	✓	✓	✓	✓	100%
ARG	✗	✗	✗	✗	✗	0%
BOL	✗	✗	✗	✗	✗	0%
BRA	✗	✗	✓	✓	✓	60%
COL	✗	✗	✗	✗	✗	0%
CRI	✗	✗	✗	✗	✗	0%
CUB	✗	✗	✗	✗	✗	0%
CHL	✓	✓	✗	✗	✓	60%
DOM	✗	✗	✓	✓	✗	40%
ECU	✓	✓	✓	✓	✓	100%
SLV	✗	✗	✗	✗	✗	0%
ESP	✓	✓	✓	✓	✓	100%
GTM	✗	✗	✗	✗	✗	0%
HND	✗	✗	✗	✗	✗	0%
MEX	✗	✗	✓	✓	✓	60%
NIC	✗	✗	✗	✓	✗	20%
PAN	✗	✗	✓	✓	✓	60%
PRY	✗	✗	✗	✗	✗	0%
PER	✗	✗	✓	✓	✓	60%
PRT	✓	✓	✓	✓	✓	100%
URY	✓	✓	✓	✓	✓	100%
VEN	✗	✗	✗	✗	✗	0%
TOTAL	27%	27%	45%	50%	45%	

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Tabla 8. Medidas proactivas para el tratamiento de datos personales en las regulaciones de los países miembros de la SEGIB (31/XII/2024)

Alternativas para realizar transferencias internacionales de datos personales en la regulación de los países miembros de la SEGIB.

Las siguientes son las principales alternativas para realizar transferencias internacionales de datos personales: Nivel adecuado de protección de datos, cláusulas contractuales, normas corporativas vinculantes, mecanismos de certificación, autorización de la autoridad de control o del titular del dato y tratados internacionales.

Lo siguiente se destaca del análisis comparativo:

- En buena parte de las regulaciones se consagra la autorización del titular del dato (64%) y los tratados internacionales (59%).
- En muy pocas regulaciones se mencionan expresamente las cláusulas contractuales y el nivel adecuado del país receptor y la autorización de la autoridad de protección de datos (50%)
- Solo el 41% prevé las normas corporativas vinculantes y la autorización de la autoridad de control. El 27% menciona los mecanismos certificación.
- Únicamente el 18,18% de los países incluyen en su regulación el 100% de las alternativas para efectuar transferencias internacionales de datos.

Lo anterior se ilustra en esta tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Alternativas para realizar transferencias internacionales según las regulaciones de los países miembros de la SEGIB								
	Nivel adecuado de protección de datos	Clausulas contractuales	Normas corporativas vinculantes	Mecanismos de certificación	Autorización de autoridad de control	Autorización de titular del dato	Tratados internacionales	%
AND	✓	✓	✓	✓	✓	✓	✓	100%
ARG	✓	✓	✓	✗	✓	✓	✓	86%
BOL	✗	✗	✗	✗	✗	✗	✗	0%
BRA	✓	✓	✓	✓	✓	✓	✓	100%
COL	✓	✗	✓	✗	✓	✓	✓	71%
CRI	✗	✗	✗	✗	✗	✓	✗	14%
CUB	✓	✗	✗	✗	✓	✓	✓	57%
CHL	✓	✓	✓	✓	✗	✓	✓	86%
DOM	✗	✓	✗	✗	✗	✓	✓	43%
ECU	✗	✓	✓	✓	✓	✓	✓	86%
SLV	✗	✗	✗	✗	✗	✗	✗	0%
ESP	✓	✓	✓	✓	✓	✓	✓	100%
GTM	✗	✗	✗	✗	✗	✗	✗	0%
HND	✗	✗	✗	✗	✗	✗	✗	0%
MEX	✓	✓	✓	✓	✗	✓	✓	86%
NIC	✗	✗	✗	✗	✗	✗	✗	0%
PAN	✗	✓	✗	✗	✗	✗	✗	14%
PRY	✗	✗	✗	✗	✗	✗	✗	0%
PER	✓	✓	✗	✗	✗	✓	✓	43%
PRT	✓	✓	✓	✓	✓	✓	✓	100%
URY	✓	✗	✗	✗	✓	✓	✓	57%
VEN	✗	✗	✗	✗	✗	✗	✗	0%
TOTAL	50%	50%	41%	32%	41%	64%	59%	

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Tabla 9. Alternativas para realizar transferencias internacionales de datos personales según las regulaciones de los países miembros de la SEGIB (31/XII/2024)

Características que deben tener las autoridades de protección de datos personales según la regulación de los países miembros de la SEGIB

Los principales requisitos que deben tener las autoridades de control o de protección de datos son: autonomía, imparcialidad, independencia, ser ajenas a toda influencia externa, tener poderes o facultades de investigación y sanción, contar con suficientes recursos humanos y materiales para cumplir sus funciones, así como contar con competencia técnica en su equipo humano.

Del análisis comparativo sobresale lo que sigue a continuación:

- En buena parte de las regulaciones (68%) se consagra la necesidad de que las autoridades tengan poderes o facultades de investigación y sanción.
- En muy pocas normas se menciona expresamente la autonomía (50%) y que la autoridad sea independiente (36%)
- El 32% de las normas establece que las autoridades deben ser imparciales y el 27% que deben contar con suficientes recursos humanos y materiales para cumplir sus funciones.
- Sólo el 23% de las regulaciones estableces que las autoridades de control deben ser ajenas a toda influencia externa.
- Únicamente el 13,63% de los países incluyen en su regulación el 100% de características de las autoridades de protección de datos.

Lo anterior se puede verificar en esta tabla:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Requisitos de las autoridades de datos según las regulaciones de los países miembros de la SEGIB

	Autonomía	Imparcialidad	Independencia	Ajena a toda influencia externa	Poderes de investigación, sanción y otros	Recursos humanos y materiales para cumplir funciones	%
AND	✓	✓	✓	✓	✓	✓	100%
ARG	✓	✗	✓	✓	✓	✗	67%
BOL	✗	✗	✗	✗	✗	✗	0%
BRA	✓	✓	✗	✗	✓	✓	67%
COL	✗	✗	✗	✗	✓	✗	17%
CRI	✓	✗	✓	✗	✓	✓	67%
CUB	✗	✗	✗	✗	✓	✗	17%
CHL	✓	✗	✗	✗	✓	✗	33%
DOM	✗	✗	✗	✗	✓	✗	17%
ECU	✓	✓	✓	✗	✓	✗	67%
SLV	✗	✗	✗	✗	✗	✗	0%
ESP	✓	✓	✓	✓	✓	✓	100%
GTM	✗	✗	✗	✗	✗	✗	0%
HND	✗	✗	✗	✗	✗	✗	0%
MEX	✓	✓	✓	✓	✓	✗	83%
NIC	✗	✗	✗	✗	✗	✗	0%
PAN	✗	✗	✗	✗	✓	✗	17%
PRY	✗	✗	✗	✗	✗	✗	0%
PER	✓	✗	✗	✗	✓	✓	50%
PRT	✓	✓	✓	✓	✓	✓	100%
URY	✓	✓	✓	✗	✓	✗	67%
VEN	✗	✗	✗	✗	✗	✗	0%
TOTAL	50%	32%	36%	23%	68%	27%	

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Tabla 10. Requisitos de las autoridades de control o protección de datos personales en las regulaciones de los países miembros de la SEGIB (31/XII/2024)

Desafíos derivados de las neurotecnologías, la inteligencia artificial y el internet de las cosas respecto del tratamiento de datos personales

Desde la década de los setenta, mediante la resolución 3384 de 1975[66], la Organización de las Naciones Unidas (ONU) se ha reconocido que "el progreso científico y tecnológico se ha convertido en uno de los factores más importantes del desarrollo de la sociedad humana" porque "crea posibilidades cada vez mayores de mejorar las condiciones de vida de los pueblos y las naciones". Pero, al mismo tiempo, "puede en ciertos casos dar lugar a problemas sociales, así como amenazar los derechos humanos y las libertades fundamentales del individuo". Concretamente, señala dicha resolución que "los logros científicos y tecnológicos pueden entrañar peligro para los derechos civiles y políticos de la persona o del grupo y para la dignidad humana".

Por eso, es inaplazable adoptar medidas para evitar las eventuales consecuencias negativas de algunos desarrollos tecnológicos frente a la sociedad en general, los derechos humanos y la dignidad

[66] Proclamada por la Asamblea General en su resolución 3384 (XXX), de 10 de noviembre de 1975 sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad. El texto oficial puede consultarse en: https://www.ohchr.org/es/instruments-mechanisms/instruments/declaration-use-scientific-and-technological-progress-interests

Con el apoyo de:
Con el apoyo de:
Cooperación Española

humana[67]. En línea con lo anterior, en la precitada resolución se acuerda, entre otros, lo que sigue a continuación:

> "7. **Todos los Estados adoptarán las medidas necesarias, incluso de orden legislativo a fin de asegurarse de que la utilización de los logros de la ciencia y la tecnología contribuya a la realización más plena posible de los derechos humanos y las libertades fundamentales** sin discriminación alguna por motivos de raza, sexo, idioma o creencias religiosas. (Destacado)
>
> "8. **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**." (Destacado)

En suma, se debe evitar que las tecnologías se utilice en detrimento del ser humano, sus derechos, la dignidad humana, la sociedad y la humanidad.

Desafíos comunes o generales de las neurotecnologías, la inteligencia artificial y el internet de las cosas respecto del tratamiento de datos personales

Existen retos comunes frente al tratamiento de datos personales mediante cualquier tecnología como, entre otras, la inteligencia artificial, el internet de las cosas, las neurotecnologías.

[67] Remolina Angarita, Nelson (2024) Neuro reflexión : hacia una Declaración Universal sobre las neurotecnologías y los derechos humanos. Artículo publicado en el libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 224

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Las tecnologías son una herramienta para recolectar, usar, circular o, en general, tratar datos personales. Por ende, el uso de las mismas debe ser respetuoso de las normas sobre tratamiento de datos personales.

En línea con lo anterior, estos son algunos desafíos generales:

- Impedir que las tecnologías se utilicen en detrimento de los derechos humanos, las libertades fundamentales y la dignidad de la persona humana[68]
- Lograr que los responsables o encargados del tratamiento cumplan la regulación sobre tratamiento de datos personales
- Garantizar los derechos de las personas frente al tratamiento de su información
- Evitar: (i) tratamientos fraudulentos o engañosos; (ii) daños a las personas y a la sociedad en general.

Al mismo tiempo, existen desafíos particulares respecto del tratamiento de datos de algunos sujetos (como los menores de edad) o del uso de algunas tecnologías. En las siguientes líneas nos referiremos a los mismos:

Desafíos de las neurotecnologías

[68] Este reto general es tomado de la Resolución 3384 del 10 de noviembre de 1975 de la ONU sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad.

Las neuro tecnologías se definen como "*métodos, herramientas o dispositivos para registrar la actividad cerebral o para cambiarla*"[69]. Señala Rafael Yuste, Profesor del Departamento de Biología de la Universidad de Columbia y Director del Proyecto BRAIN, que "*La neurotecnología es importante porque el cerebro no es un órgano más del cuerpo, sino el órgano que genera toda la actividad mental y cognitiva de los seres humanos. Nuestros pensamientos, nuestras percepciones, nuestras emociones, nuestras memorias, incluso el subconsciente…todo surge de la actividad coordinada de circuitos neuronales dentro de nuestro cerebro. Y con la neurotecnología, por primera vez podemos adentrarnos en estos circuitos neuronales, registrar su actividad y cambiarla*" [70].

El citado científico pone de presente los beneficios del uso de neurotecnologías como, entre otros, los siguientes: (i) realizar "investigaciones para descubrir cómo funciona el cerebro y cuál es la base científica de la mente humana" [71]; (2) "diagnosticar, entender, y diseñar nuevas terapias para las enfermedades cerebrales tanto neurológicas, neurodegenerativas o psiquiátricas. Enfermedades como el Alzheimer, la esquizofrenia, el Parkinson, la epilepsia, la discapacidad mental, el ictus, la esclerosis lateral, la depresión, la ansiedad, etc… Estas enfermedades cerebrales afectan de una manera cada vez mayor a un gran porcentaje de los ciudadanos y son la lacra de la humanidad" [72]; y (3) Fomentar "la creación de dispositivos de interfaz cerebro computadora, que permitan la

[69] Cfr. Yuste, Rafael (2024) Un paso histórico. Presentación del libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 7

[70] Cfr. Yuste, Rafael (2024) Un paso histórico. Presentación del libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 7

[71] Cfr. Yuste, Rafael (2024) Un paso histórico. Presentación del libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 7

[72] Cfr. Yuste, Rafael (2024) Un paso histórico. Presentación del libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 7-8

conexión directa con el internet, y forme la base de una industria nueva, con grandes beneficios económicos y también a los consumidores" [73].

Retos o desafíos

No obstante lo anterior, las neuro tecnologías también generan riesgos como, entre otros, los siguientes:

- **Usar las neurotecnologías para fines contrarios a la dignidad humana**. Con éstas se puede descodificar y alterar la actividad cerebral, lo cual genera problemas/retos éticos, jurídicos y sociales muy profundos ya que se podría cambiar la esencia del ser humano y manipularlo / alterarlo.
- **Modificar artificialmente los seres humanos**. Los hallazgos científicos en neurociencias y su aplicación a través de diversas neuro tecnologías tienen el potencial de alterar algunas características humanas fundamentales, como la autonomía, la responsabilidad moral, el libre albedrío, la dignidad, la identidad, la vida mental privada, la comprensión de los individuos como entidades atadas por sus cuerpos, la integridad y la seguridad corporal. [74]
- **Generar daños físicos al ser humano y la manipulación mental.** También pueden producir daños físicos asociados con los procedimientos invasivos de colocación de los dispositivos

[73] Cfr. Yuste, Rafael (2024) Un paso histórico. Presentación del libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 8

[74] Yuste, Rafael; Goering, Sara; Bi, Guoqiang; Carmena, José M.; Carter, Adrian; Fins, Joseph J. ... & Wolpaw, Jonathan (2017). Four ethical priorities for neurotechnologies and AI. Nature News, 551 (7679), 159-163.

para mejoramiento o para la interfaz cerebro-máquina. daño tisular y deterioro de la función motora (vulneración al derecho a la integridad mental).[75]

- **Indebido tratamiento de los neurodatos y uso de los mismos para fines contrarios a la dignidad humana o no autorizados por la ley**. El "secuestro cerebral" puede implicar el robo de información (violación del derecho a la privacidad mental). También existe la posibilidad de ingreso de virus, o que los dispositivos neuronales conectados a internet posibiliten que individuos u organizaciones (hackers, corporaciones o agencias gubernamentales) rastreen o, incluso, manipulan la experiencia mental de un individuo[76]

Para resumir, pese a los beneficios en la salud mental que traerán las neurotecnologías, existe el temor que con la neurodata se pueda, no sólo conocer lo que piensan las personas (que por ahora es un secreto), sino manipular cerebralmente seres humanos. Por eso, desde hace poco se vienen gestando los neuroderechos que tienen como finalidad lo siguiente:

- No perder la privacidad que tenemos respecto de nuestro cerebro (lo que pensamos)
- Derecho a ser como soy: derecho al yo, a mi identidad cerebral natural.
- Derecho a decidir por mí mismo, sin ser artificialmente manipulado o programado
- Neurotecnologías neutrales. No sesgadas. Que no se implanten sesgos en nuestro cerebro.
- Acceso equitativo a las neurotecnologías

La Red Iberoamericana de protección de datos ha planteado que "Los datos cerebrales o neurodatos muestran ciertas características como son:

[75] Yuste, Rafael; Goering, Sara; Bi, Guoqiang; Carmena, José M.; Carter, Adrian; Fins, Joseph J. ... & Wolpaw, Jonathan (2017). Four ethical priorities for neurotechnologies and AI. Nature News, 551 (7679), 159-163.

[76] Yuste, Rafael; Goering, Sara; Bi, Guoqiang; Carmena, José M.; Carter, Adrian; Fins, Joseph J. ... & Wolpaw, Jonathan (2017). Four ethical priorities for neurotechnologies and AI. Nature News, 551 (7679), 159-163.

- La información del sistema nervioso y del cerebro es única y personal. En particular, cada cerebro humano es único y permite la identificación personal a través de la anatomía de las regiones cerebrales. El cerebro es una seña de identidad tan inconfundible como la huella dactilar. Por ello, los autores que han tratado esta materia concluyen que las estructuras de todo el sistema nervioso, y de forma precisa, el cerebro humano es exclusiva de los individuos y pueden utilizarse para la identificación de sujetos.
- Los neurodatos pueden permitir una profundidad y una forma únicas de comprensión del individuo, pudiendo usarse de manera predictiva, para descubrir características o predisposiciones que pueden no ser conocidas por el individuo. Y pueden permitir conocer los procesos cerebrales en "tiempo real", lo que permite el registro directo de procesos asociados con la personalidad, el estado de ánimo, los comportamientos, los pensamientos o los sentimientos."[77]

Durante 2024, la RIPD aprobó la Declaración sobre neurotecnologías y neurodatos dentro del marco del encuentro de la Red Iberoamericana de Protección de Datos, el cual se realizó en la ciudad de Cartagena (Colombia) del 27 al 29 de mayo de 2024. El documento es de gran importancia porque, entre otras, se enfoca en analizar los desafíos de la neurotecnologías desde la óptica del tratamiento de los datos personales.

En la citada declaración, la RIPD, hace lo siguiente:

1. Define los neurodatos y reafirma su naturaleza de datos pesonales cuando estén asociados a personas identificadas o identificables. Y destaca que el cerebro será un identificador tan único como la huella dactilar o el genoma" y que "los avances técnicos y científicos no se encuentran libres de errores, tendencias, sesgos, interpretaciones políticas o religiosas o prejuicios, por lo que puede llevar a situaciones de neurodiscriminación." Por ende,

[77] Cfr. RIPD, 2023. Declaración sobre neurodatos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en la Antigua, Guatemala el 25 de septiembre de 2023.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

concluye la RIPD, "todo tratamiento que incluya neurodatos se considerará un tratamiento de alto riesgo de datos personales" [78]

2. Exige que debería existir un marco específico de transparencia en el tratamiento de neurodatos que permita "posibilitar el debate público, asegurar la rendición de cuentas y la exigencia de responsabilidades a actores públicos y privados, así como garantizar el ejercicio de derechos a todos los afectados, en un ecosistema complejo y supranacional"[79]
3. Demanda que existan garantías específicas sobre los neurodatos en razón a los riesgos asociados al tratamiento de esa información.[80]
4. Establece factores que deben tenerse presente para establecer la responsabilidad del productor, proveedor o administrador de las neurotecnologías.[81]
5. Recuerda la propuesta de crear nuevos neuroderechos, a saber: a) Identidad personal,; b) Libre albedrío; c) Privacidad mental; d) Acceso equitativo, y e) Protección contra sesgos.[82]

---

[78] Cfr. RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024). Págs. 2 y 3

[79] Cfr. RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024). Pág. 3

[80] Cfr. RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024). Págs. 4 y 5

[81] Cfr. RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024). Págs. 5

[82] Cfr. RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024). Págs. 5 y 6

Desafíos de la inteligencia artificial (IA)

Existen diferentes definiciones sobre inteligencia artificial (en adelante IA). No obstante como punto de partida tomaremos la siguiente que usualmente se cita en documentos sobre IA y por organizaciones como la OCDE, la UE, el CdE, a saber: IA es "es un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de las entradas que recibe, cómo generar salidas tales como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después de su implementación"[83].

La RIPD, por su parte, ha señalado que la AI es un "término "*sombrilla*" que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de *machine learning*, hasta llegar a las técnicas de *deep learning*. Particularmente se vincula el uso de algoritmos a la IA, los cuales son un conjunto de reglas o una secuencia de operaciones lógicas que proporcionan instrucciones para que las máquinas tomen decisiones o actúen de determinada manera"[84]

[83] Cfr. OCDE, 2024. AI, data governance and privacy synergies and areas of international cooperation. OCDE Artificial Intelligence papers. June, no. 22. Pág 27. En: https://doi.org/10.1787/2476b1a4-en .

[84] Cfr. RIPD, 209. Recomendaciones generales para el tratamiento de datos en la inteligencia artificial. Pág 6

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Finalmente, en el numeral 1 del artículo 3 del Reglamento Europeo de Inteligencia Artificial (REIA) se definen lo sistemas de IA de la siguiente manera: “ “«sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;”[85]

Usualmente, se enuncian los siguientes retos del tratamiento de datos mediante herramientas de IA: En primer lugar, los riesgos en los algoritmos y en la información que estos procesan. La información puede carecer de calidad (datos parciales, insuficientes o desactualizados) que afectan la precisión y relevancia de los resultados. En segundo lugar, las fallas algorítmicas porque los algoritmos pueden ser influenciados por fallas técnicas, sesgos en la lógica de programación o errores en las condiciones de operación. Finalmente, la carencia de transparencia y explicabilidad para proteger la humanidad y los derechos humanos, especialmente en la toma de decisiones que afectan a las personas.

[85] Cfr. UE (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

La ONU se refirió a los principios de transparencia y explicabilidad en la inteligencia artificial, mediante el Informe A/78/310 del 30 de agosto de 2023, en donde recalcó la importancia de citados principios en el tratamiento de datos personales mediante la inteligencia artificial[86].

Lo anterior es relevante 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 estos principios, de 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, de otra parte, se exige que las personas afectadas por la inteligencia artificial conozcan los motivos concretos que dieron origen a dicha afectación. Con esto, la persona podrá ejercer sus derechos como, por ejemplo, al debido proceso y el derecho de defensa frente a las decisiones adoptadas mediante herramientas o tecnologías de inteligencia artificial.

En el informe se recalcó que la inteligencia artificial involucra diferentes tipos de riesgos. Entre las contingencias a tener en cuenta deben considerarse, entre otras, 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.

En cuanto a los datos personales, se recordó que los mismos son un insumo que procesan los algoritmos para arrojar resultados. Los datos de entrada pueden 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 y pertinentes, los resultados serán erróneos . El algoritmo, por su parte, puede ser 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, los cuales están relacionados

[86] Cfr. ONU. Informe A/78/310 del 30 de agosto de 2023: 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, Ana Brian Nougrères.. En: https://www.ohchr.org/es/documents/thematic-reports/a78310-principles-transparency-and-explainability-processing-personal

Con el apoyo de:
Con el apoyo de:
Cooperación Española

con la pertinencia y precisión del resultado de la ejecución del algoritmo y como respuesta al análisis de los datos de entrada

En el informe se concluyó, entre otras, lo siguiente:

> "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 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." [87]

Adicionalmente, se formularon las siguientes recomendaciones:

[87] Cfr. ONU. Informe A/78/310 del 30 de agosto de 2023. Págs 20-21.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

"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." [88]

Finalmente, y no menos importante, nn el informe ONU A/HRC/46/37 del 25 de enero de 2021 sobre inteligencia artificial y la privacidad, así como la privacidad de los niños, se señaló lo siguiente respecto de la inteligencia artificial:

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"[89].

[88] Cfr. ONU. Informe A/78/310 del 30 de agosto de 2023. Pág 21.
[89] Cfr. ONU. Informe A/HRC/46/37 del 25 de enero de 2021. Pág. 2 .

Allí se puso de presente que tanto el tratamiento de los datos como la decisión que se adopte como resultado de ese tratamiento mediante herramientas de inteligencia artificial (IA) entrañan riesgos potenciales para los titulares de datos. Por eso, se consideró importante establecer unos principios relevantes a la hora de planificar, desarrollar y aplicar soluciones de IA. Dichos principios son los siguientes: 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.

Algunos lineamientos del Reglamento Europeo de Inteligencia Artificial (REIA)

El Reglamento Europeo de Inteligencia Artificial (en adelante REIA) [90] del 13 de junio de 2024 es un referente mundial en regulación sobre inteligencia artificial (IA).[91]

El REIA busca, entre otras, que las herramientas de IA sean fiables, éticas, seguras, respetuosas de los derechos humanos y centradas en el ser humano. Puntualmente, señala numeral 1 del artículo 1 del citado reglamenteo que el mismo tiene como objetivo "(…) promover la adopción de una

[90] Cfr. El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE)

[91] Como lo mencionamos, el REIA define la IA como "un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales" (Cfr. Numeral 1 del artículo 3 del REIA)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión así como prestar apoyo a la innovación."

En línea con lo anterior, el numeral 2 del citado artículo se enuncian los principales temas que regula el REIA:

a) Prohibiciones de determinadas prácticas de IA;
b) Requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;
c) Normas armonizadas :
- para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión;
- de transparencia aplicables a determinados sistemas de IA;
- para la introducción en el mercado de modelos de IA de uso general;
d) Normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento;
e) Medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.

El REIA es un texto extenso de 113 artículos y 68 definiciones[92] que aborda detalladamente muchos temas. Dado lo anterior, solo nos centraremos en ciertos aspectos relacionados con el tratamiento de datos y la IA.

Prácticas prohibidas

[92] Cfr. Artículo 3 del REIA

El REIA prohíbe prácticas que:

1. Manipulen el ser humano o un colectivo de personas[93]
2. Exploten negativamente las vulnerabilidades de una persona o un colectivo de personas[94]
3. Evalúen o clasifiquen personas físicas o colectivos de personas bajo determinadas circunstancias y que generen ciertos resultados o efectos.[95]
4. Realicen evaluaciones de riesgos de personas con miras a valorar o predecir el riesgo de que una persona física cometa un delito[96]
5. Creen o amplíen bases de datos de reconocimiento facial mediante determinados procedimientos [97]
6. Infirieran las emociones de una persona física en los lugares de trabajo y en los centros educativos[98]
7. Clasifiquen a las personas físicas sobre la base de sus datos biométricos para ciertos fines. [99]
8. Realicen, salvo algunas excepciones, identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho. [100]

El artículo 5 enuncia una serie de prácticas que prohíben que la IA use técnicas que manipulen el ser humano[101] como las siguientes:

- **Técnica subliminales** que trasciendan la conciencia de una persona, o
- **Técnicas deliberadamente manipuladoras o engañosas** con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas,

[93] Cfr. Literal a) del artículo 5 del REIA
[94] Cfr. Literal b) del artículo 5 del REIA
[95] Cfr. Literal c) del artículo 5 del REIA
[96] Cfr. Literal d) del artículo 5 del REIA.
[97] Cfr. Literal e) del artículo 5 del REIA
[98] Cfr. Literal f) del artículo 5 del REIA
[99] Cfr. Literal g) del artículo 5 del REIA
[100] Cfr. Literal h) del artículo 5 del REIA.
[101] Cfr. Literal a) del artículo 5 del REIA

Con el apoyo de:
Con el apoyo de:
Cooperación Española

mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

Adicionalmente, prohíbe el uso de IA que:

- **Explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas** derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra; [102]
- **Evalúe o clasifique a personas físicas** o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:
    - i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;
    - ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este; [103]
- **Realice evaluaciones de riesgos de personas físicas** con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad;[104]

[102] Cfr. Literal b) del artículo 5 del REIA
[103] Cfr. Literal c) del artículo 5 del REIA
[104] Cfr. Literal d) del artículo 5 del REIA. "Esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva"

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- **Cree o amplíe bases de datos de reconocimiento facial** mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;[105]
- **Infiriera las emociones de una persona física en los lugares de trabajo y en los centros educativos**, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad; [106]
- **Clasifique individualmente a las personas físicas sobre la base de sus datos biométricos** para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; [107]
- **Realice identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho**, salvo y en la medida en que dicho uso cumpla unos requisitos y sea estrictamente necesario para alcanzar uno o varios objetivos relacionados con la búsqueda de víctimas de algunos delitos, la prevención de atentados terroristas o la captura de personas sospechosas de haber cometido un delito. [108]

Evaluación de impacto relativa a los derechos fundamentales y derecho de explicabilidad

[105] Cfr. Literal e) del artículo 5 del REIA
[106] Cfr. Literal f) del artículo 5 del REIA
[107] Cfr. Literal g) del artículo 5 del REIA. "Esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho"
[108] Cfr. Literal h) del artículo 5 del REIA.Los objetivos permitidos son los siguientes:" i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas, ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista, iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos que tengan como sanción una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años."

Con el apoyo de:
Con el apoyo de:
Cooperación Española

El REIA propende por un enfoque preventivo de la IA. Para efectos de lo anterior ordena que antes de desplegar sistemas de IA de alto riesgo, se debe realizar una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales.

En lo referente a los derechos humanos y el tratamiento de datos personales, el artículo 27 del REI señala que la evaluación debe contener, entre otras, lo siguiente:

- Las categorías de personas físicas y colectivos que puedan verse afectados la utilización de la IA
- Los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos
- Las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.
- Una descripción de la aplicación de medidas de supervisión humana, cuo objetivo es "prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan" [109]

Este estudio es complementario a la evaluación de impacto de protección de datos a que se refiere al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680.

De otra parte, en el artículo 86 del REIA se consagra el derecho de "a explicación de decisiones tomadas individualmente" para que a una persona se le den "explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada". Este derecho puede ejercerlo la persona afectada por una decisión que se adopte basándose en los resultados de salida de un sistema de IA de alto riesgo, y "que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales"

[109] Cfr. Numeral 2 del artículo 14del REIA.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Desafíos en torno a la protección de los menores en entornos digitales con relación al tratamiento de los datos personales

Cada día aumenta el uso de servicios digitales, portales *web*, redes sociales y aplicaciones tecnológicas por parte de los niños, niñas y adolescentes (en adelante NNA). Los NNA son personas altamente influenciadas por la tecnología, internet y las redes sociales[110].

Los menores de edad tienen acceso a internet a través de celulares, tabletas y computadores. La aparición de las redes sociales, los juegos en línea y los espacios de aprendizaje en internet, han abierto nuevos escenarios de interacción para los niños, niñas y adolescentes. El acceso y uso de esas herramientas requieren de los datos personales de los NNA, que son recolectados, usados o tratados por empresas, personas y entidades públicas ubicadas en diferentes partes del mundo.

Adicionalmente, los menores de edad comparten su información personal ignorando los peligros a los que se exponen al suministrar sus Datos y la información de terceros (amigos, compañeros de colegio, su familia) en plataformas web de manera indiscriminada. Nombres; apellidos; fotos; videos; comentarios; la edad; los gustos y preferencias; Datos como correo electrónico; entre otros, son compartidos por los menores de edad sin pensar que estos hacen parte de su información personal y privada, que hace parte de su identidad digital. Tampoco tienen presente que una vez difunde su información en internet perderán control de la misma.

[110] Recomendaciones tomadas de: SIC, 2021. Guía cuida tu identidad digital y protege tus datos personales: riesgos sobre el tratamiento de datos personales de niños, niñas y adolescentes. En los siguientes párrafos tomares algunas partes de esta guía, cuyo autor de este estudio fue coautor de la misma.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Es clave que los menores de edad protejan sus Datos personales toda vez que estos hacen parte de su identidad y un uso inadecuado puede causar daños en la intimidad, honra y buen nombre, no solo de ellos mismo sino de otras personas. El menor de edad debe reflexionar sobre su seguridad y comprender que es el encargado de proteger su identidad digital y de preservar el buen nombre de los otros en línea.

Todo lo que se hace en internet deja huella y una vez se pone información en la red se pierde control sobre la misma porque puede ser recolectada y usada por terceros. Igualmente, cada vez que los NNA se registran en las redes sociales, en páginas de internet, aplicaciones o en las páginas de juegos en línea, están creando una identidad digital a partir de sus Datos personales.[111]

Progresivamente han aumentado los casos que evidencian los riesgos y peligros a los que se ven expuestos los NNA en las redes sociales digitales. Se ha puesto de presente que *"Los niños, niñas y adolescentes tienen cada vez mayor acceso a los distintos sistemas de comunicación, que les permiten obtener todos los beneficios que ellos representan, pero esta situación también ha llevado al límite el balance entre el ejercicio de los derechos fundamentales y los riesgos —para la vida privada, el honor, buen nombre, y la intimidad, entre otros— que, así como los abusos de los cuales pueden ser víctimas —como discriminación, explotación sexual, pornografía, entre otros— pueden tener un impacto negativo en su desarrollo integral y vida adulta"*[112]

Finalmente, se ha enfatizado en la necesidad de proteger "*la información personal de niñas, niños y adolescentes sin que se afecte su dignidad como personas ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran*

[111] Cfr. Sanz, J., 2020. *Sé legal en internet.* Agencia Española para la Protección de Datos.
[112] Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes - Memorandum de Montevideo- (2009). En: http://www.iijusticia.org/Memo.htm#_ftnref6

Con el apoyo de:
Con el apoyo de:
Cooperación Española

que se encuentran en un espacio privado" [113] . Es muy importante no perder de vista lo anterior, pues, a partir de la información que existen sobre NNA en internet o redes sociales digitales se crea la identidad digital de aquellos, la cual incide en su presente y futuro como seres humanos.

Algunos riesgos o peligros

Progresivamente han venido aumentado los casos que evidencian los riesgos y peligros a que se ven expuestos las NNA que interactúan en las redes sociales digitales y otros canales digitales. Esas redes y tecnologías, por sí solas no son el problema, pero, infortunadamente, algunas personas han encontrado en las mismas un escenario perfecto para realizar conductas indebidas. El acoso sexual "grooming", el acoso online "ciberbullying", los chantajes, la pornografía, las amenazas e invasiones de su privacidad están al orden del día.

A continuación, se explican los principales peligros a los cuales están expuestos los NNA en las redes. Dichos riesgos deben ser conocidos por los menores para que estos sean conscientes de los riesgos que pueden encontrar al ingresar a aplicaciones, redes sociales, páginas web o páginas de juegos en línea.

· **Ciberbullying o Troleo**

[113] Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes - Memorandum de Montevideo- (2009). En: http://www.iijusticia.org/Memo.htm#_ftnref6

El ciberbullying es el uso de las redes sociales o plataformas digitales para humillar, difamar o acosar a una persona. Es una manera de maltrato que puede ocasionar daños físicos y psicológicos. El troleo, por su parte, es la provocación a otros mediante insultos u obscenidades.

- **Grooming**

El grooming es uno de los principales peligros a los que se exponen los NNA en internet, este ocurre principalmente en las redes sociales. Se refiere a todas las acciones que realiza un adulto para ganar la confianza de un NNA para acosarlo o abusar sexualmente de este.[114]

Algunos adultos crean perfiles falsos y ganan la confianza de los menores de edad a través de mensajes. Los adultos se hacen pasar por otros niños, niñas o jóvenes y engañan a los menores de edad. También se da a través de los juegos en línea. Muchas páginas de juegos en internet requieren que los NNA creen un perfil. Los adultos se inscriben en estos juegos para interactuar con los menores de edad y engañarles.

- **Sexting**

El sexting es el envío de fotografías o videos íntimos que hace una persona de sí misma con contenido sexual. Es una práctica común entre los adultos, pero practicada por muchos

[114] Cfr. Sanz, J., 2020. *Sé legal en internet.* Agencia Española para la Protección de Datos.

adolescentes.[115] Se considera una práctica riesgosa, ya que la mayoría de las veces quien manda un contenido de este tipo confía que la persona que lo reciba no lo compartirá con nadie más.

Sin embargo, en ocasiones lo que sucede es que el contenido termina en manos de un tercero o en publicaciones en línea. Estos contenidos se pueden utilizar para extorsionar o chantajear a las personas y sacar un beneficio propio, esto se conoce como sextorsión. Los menores pueden conocer personas a través de internet que pueden pedir fotografías y videos con contenidos sexuales para luego atentar contra su dignidad y su honra. Estas publicaciones pueden terminar en páginas en internet de contenido sexual, lo cual constituye un delito ya que esto se consideraría pornografía infantil.

· **Suplantación de Identidad**

Suplantar significa, entre otras, *"ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba"*[116]; *"sustituir ilegalmente a una persona u ocupar su lugar para obtener algún beneficio"*[117]. La suplantación de identidad consiste en hacerse pasar por otra persona para diversos propósitos: engañar a terceros, obtener bienes y servicios con cargo a la persona suplantada, incurrir en fraudes y otro de conductas ilícitas.

Mediante la suplantación de identidad los impostores engañan a terceros, obtienen créditos, adquieren productos o servicios en nombre de la persona suplantada y ésta última es la afectada porque, en muchos casos, le toca asumir el pago de dichas obligaciones.

[115] Cfr. Sanz, J., 2020. *Sé legal en internet.* Agencia Española para la Protección de Datos.
[116] Cfr. Diccionario de la lengua española. Actualización 2017. http://dle.rae.es/?id=YlZNKd0
[117] Cfr. WordReference.com: http://www.wordreference.com/definicion/suplantar

La suplantación, se puede dar entre pares o por parte de un adulto a un menor de edad. Es probable que, tratándose de menores de edad, el hurto de identidad se dé en las redes sociales. Los NNA pueden hacerse pasar por sus amigos y compañeros creando perfiles con sus nombres y fotos a modo de broma o a modo de bullying o troleo. En este sentido, es preciso recalcar que los Datos no se deben usar en nombre de nadie y sin su Autorización o consentimiento.

Por otro lado, se puede dar la suplantación cuando un adulto hurta la identidad de un menor de edad y se hace pasar por este para obtener información personal de él o con a el fin de acosar a otros NNA. Cuando el menor de edad le entrega sus Datos a desconocidos en internet, o no es cauteloso con el manejo de su información, queda expuesto a que la persona que adquiera la adquiera, le suplante y la use para fines ilícitos como el acoso, chantaje o extorsión.

En el precitado informe ONU A/HRC/46/37 del 25 de enero de 2021 sobre inteligencia artificial y la privacidad, así como la privacidad de los niños, se señaló lo siguiente:

En primer lugar, respecto de la privacidad de los niños se concluyó que es necesario, entre otros, aprobar políticas, legislación y normas que:

i) “Consideren a los niños como titulares de derechos humanos, con un derecho inalienable a la intimidad, la autonomía y la igualdad;

ii) Incorporen el alcance general de la privacidad, y no sólo en relación con la protección de datos, para permitir el pleno desarrollo del potencial de los niños;

iii) 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;

Con el apoyo de:
Con el apoyo de:
Cooperación Española

iv) 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" [118]

Adicionalmente, 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 adecuada" [119]

[118] Cfr. ONU. Informe A/HRC/46/37 del 25 de enero de 2021: La inteligencia artificial y la privacidad, así como la privacidad de los niños - Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci. Pág. 22 . En: https://www.ohchr.org/es/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy
[119] Cfr. ONU. Informe A/HRC/46/37 del 25 de enero de 2021. Pág. 24 .

Del anteproyecto de ley del Reino de España para la protección de las personas menores de edad en los entornos digitales

El 11 de junio se presentó en España un proyecto de ley cuyo objetivo es "establecer medidas con la finalidad de garantizar la protección de las personas menores de edad en los entornos digitales"[120]. Se trata de una iniciativa regulatoria que busca la adopción de un "conjunto integral de medidas en distintos ámbitos (protección de los consumidores, educativo, sanitario, legislación penal, sector audiovisual, …) orientadas a un mejor uso de estos medios digitales con el fin de proteger a las personas menores de edad en el entorno digital" [121]

[120] Cfr. Artículo 1 del ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES, elaborada por los siguientes ministerios de España: Ministerio de la presidencia, justicia y relaciones con las cortes ; Ministerio de juventud e infancia; Ministerio para la transformación digital y de la función pública, y Ministerio de derechos sociales, consumo y agenda 2030. El texto se puede consultar en: https://www.mpr.gob.es/servicios/participacion/Documents/ANTEPROYECTO%20DE%20LEY%20ORG%C3%81NICA%20PARA%20LA%20PROTECCI%C3%93N%20DE%20LAS%20PERSONAS%20MENORES%20DE%20EDAD%20EN%20LOS%20ENTORNOS%20DIGITALES.pdf

[121] Información tomada de la Memoria del análisis de impacto normativo (MAIN) sobre el ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES, elaborada por los siguientes ministerios de España: Ministerio de la presidencia, justicia y relaciones con las cortes ; Ministerio de juventud e infancia; Ministerio para la transformación digital y de la función pública, y Ministerio de derechos sociales, consumo y agenda 2030. El texto se puede consultar en: https://www.mpr.gob.es/servicios/participacion/Documents/MAIN.pdf

Con el apoyo de:
Con el apoyo de:
Cooperación Española

La propuesta reconoce los beneficios de los medios tecnológicos para la sociedad, pero destaca algunos riesgos que es necesario mitigar. En concreto, plantea que "el uso inadecuado de estos medios digitales, por las personas menores de edad, o por los adultos en relación con ellos, puede provocar importantes perjuicios a los menores y a sus familias, tales como daños psicológicos y emocionales; daños para la salud física; desinformación, manipulación y construcción de falsas creencias; establecimiento de conductas peligrosas o socialmente inapropiadas; inclusión en grupos y colectivos dañinos; adicciones; o perjuicios económicos."[122]

Dado lo anterior, el proyecto de ley tienes estas finalidades:

- "Garantizar el respeto y cumplimiento de los derechos de las niñas, niños y adolescentes en el entorno digital, especialmente los derechos a la intimidad, al honor y a la propia imagen, al secreto de las comunicaciones y a la protección de los datos personales y el acceso a contenidos adecuados a la edad.
- "Fomentar un uso equilibrado y responsable de los entornos digitales a fin de garantizar el adecuado desarrollo de la personalidad de las personas menores de edad y de preservar su dignidad y sus derechos fundamentales.
- "Garantizar que los productos y servicios digitales tengan en cuenta, desde su diseño y por defecto, el interés superior del menor.
- "Apoyar el desarrollo de las competencias digitales de la infancia en el entorno digital y la capacidad de evaluar los contenidos en línea y detectar la desinformación y el material abusivo.
- "Promover un entorno digital más seguro y estimular la investigación en este ámbito." [123]

[122] Ídem
[123] Cfr. Artículo 2 del ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES.

Adicionalmente, la propuesta incluye los siguientes derechos para los menores de edad:

- "Ser protegidas eficazmente ante contenidos digitales que puedan perjudicar su desarrollo.
- "Recibir información suficiente y necesaria en una forma y lenguaje apropiado según la edad sobre el uso de las tecnologías, así como de sus derechos y de los riesgos asociados al entorno digital.
- "Acceso a la información, a la libertad de expresión, y a ser escuchadas.
- "Acceso equitativo y efectivo a dispositivos, conexión y formación para el uso de herramientas digitales." [124]

El proyecto de ley se divide en varios títulos, cuyo contenido esencial enunciamos a continuación :

Título I. Medidas en el ámbito de la protección de los consumidores y usuarios

- ***Obligaciones de los fabricantes de dispositivos digitales con conexión a internet (artículo 4).*** Se obliga a lo siguiente a los fabricantes de dispositivos digitales que tengan la capacidad de conectarse a internet y a través de dicha conexión pueda accederse a contenidos perjudiciales para menores, como es el caso de teléfonos móviles, tabletas electrónicas, televisores inteligentes y ordenadores de uso personal:
    - Proporcionar información en sus productos en la que se advierta, en un lenguaje accesible, inclusivo y apropiado para todas las edades, de los riesgos derivados del acceso a contenidos perjudiciales para la salud y el desarrollo físico, mental y moral de los menores.
    - Facilitar información sobre las medidas de protección de datos y riesgos relacionados con la privacidad y la seguridad; el tiempo recomendado de uso de los

[124] Cfr. Artículo 2 del ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

productos y servicios, adecuado a la edad de la persona usuaria; los sistemas de control parental; los riesgos sobre el desarrollo cognitivo y emocional y la afección a la calidad del sueño de un uso prolongado de tales servicios.
    - Garantizar que los dispositivos incluyan una funcionalidad gratuita de control parental de servicios, aplicaciones y contenidos, cuya activación debe producirse por defecto en el momento de la configuración inicial del dispositivo.
    - Acreditar ante los importadores, distribuidores y comercializadores que los dispositivos suministrados cumplen los requisitos y condiciones establecidos en los párrafos anteriores. Los importadores, distribuidores y comercializadores deberán desarrollar actuaciones de verificación del cumplimiento de estos requisitos y condiciones.

- ***Regulación del acceso y activación de los mecanismos aleatorios de recompensa (artículo 5):*** Se prohibe el acceso a los mecanismos aleatorios de recompensa o su activación por personas que sean menores de edad. Dichos mecanismos son aquellos de funcionalidad virtual cuya activación se realiza con dinero de curso legal o a través de un objeto virtual, como un código, clave, in-game currency, criptomoneda u otro elemento, adquirido con dinero directa o indirectamente; en la que el resultado de dicha activación sea incierto y consista en la obtención de un objeto virtual que pueda ser canjeado por dinero o por otros objetos virtuales.

Título II. Medidas en el ámbito educativo

- ***Actividades de formación en los centros de educación infantil, primaria, secundaria obligatoria y secundaria postobligatoria (artículo 6).*** El texto imponer a las ddministraciones educativas los siguientes deberes:
    - Fomentar en los centros de educación infantil, primaria, secundaria obligatoria y secundaria postobligatoria, independientemente de su titularidad, el desarrollo de actividades encaminadas a la mejora de la competencia digital con el fin de garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro, saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, el trabajo y la participación en la sociedad, así como la interacción con estas.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Incluir, en su planificación de la formación continua del profesorado, actividades formativas que faciliten a los docentes estrategias para incidir, entre otros aspectos, en la seguridad (incluido el bienestar digital y las competencias relacionadas con la ciberseguridad) y en asuntos relacionados con la ciudadanía digital, la privacidad y la propiedad intelectual.

- ***Regulación del uso de dispositivos en los centros de educación infantil, primaria, secundaria obligatoria y secundaria postobligatoria (artículo 7):*** Se ordena a los centros de educación infantil, primaria, secundaria obligatoria y secundaria postobligatoria, regular el uso de dispositivos móviles y digitales en las aulas, en las actividades extraescolares y en lugares y tiempos de descanso que tengan lugar bajo su supervisión.

Título III. Medidas en el ámbito sanitario

- ***Prevención y promoción de la salud (artículo 8).*** Con esta disposición se busca lo siguiente:
  - Que las administraciones públicas que promuevan estudios sobre el uso de las tecnologías de información y comunicación por las personas menores de edad tengan en cuenta el principio de «salud en todas las políticas» y elaborar guías para la prevención y la promoción de la salud en el uso de las tecnologías de información y comunicación por las personas menores de edad.
  - Que los programas de prevención y de promoción de la salud infantil y juvenil de las administraciones sanitarias incorporen actuaciones para la identificación de usos problemáticos de dichas tecnologías y la detección precoz de cambios de conductas o problemas de salud física, psíquica y emocional, derivados de un uso inadecuado. En la detección precoz de situaciones de riesgo, se debe poner especial atención en identificar aquellas en las que niñas, niños y adolescentes recurran de forma prioritaria al entorno digital para entablar relaciones de pares.
  - Las administraciones sanitarias competentes deben revisar las actuaciones de prevención de trastornos adictivos para la inclusión de las adicciones sin sustancia relacionadas con el uso de medios digitales.
  - Promover la coordinación de todas las administraciones públicas y agentes implicados, especialmente de los servicios de atención primaria, atención especializada a la salud mental y a las conductas adictivas, servicios sociales y educativos. En particular, las administraciones sanitarias impulsarán la elaboración

Con el apoyo de:
Con el apoyo de:
Cooperación Española

conjunta con otras administraciones públicas de programas y circuitos de derivación para el abordaje integral de los problemas de salud detectados, así como mapas de recursos comunitarios y de activos en salud que contribuyan a un desarrollo saludable de las personas menores.
    - Facilitar la formación y la sensibilización sobre las consecuencias en la salud del uso excesivo de las tecnologías de la información y comunicación, de los y las profesionales de la salud que atienden a esta población

- ***Atención especializada (artículo 9).*** Se promueve el establecimiento de procedimientos de atención sanitaria específicos para personas menores con conductas adictivas sin sustancia en la red especializada de atención a la salud mental, tanto en las Unidades de Atención a la Conducta Adictiva, como en los centros de salud mental infantojuveniles.

Título IV. Medidas en el sector público

- ***Participación, información y sensibilización (artículo 10).*** Las administraciones públicas deberán:
    - Promover la garantía de los derechos de las personas menores de edad en el ámbito digital desde una perspectiva preventiva e integral, así como de consulta y participación de la infancia y juventud. Para ello velarán por crear contenidos digitales de calidad destinados a la promoción de hábitos saludables, el buen trato, la igualdad de género, la participación democrática y el acceso a distintos formatos de cultura.
    - Promover espacios de interlocución con niños y adolescentes para conocer su experiencia con las tecnologías de la información y comunicación, así como para diseñar de forma participativa iniciativas relativas a la promoción cultural en el entorno digital.
    - Desarrollar campañas y actividades de sensibilización, concienciación, prevención e información sobre los riesgos asociados al uso inadecuado de los entornos y dispositivos digitales, prestando especial atención al consumo de material pornográfico.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Promover la realización de estudios e investigaciones sobre la prevalencia del acoso y la violencia en sus diferentes ámbitos en los entornos digitales.
- Impulsar la puesta a disposición de la infancia y adolescencia de espacios de encuentro en los que puedan desarrollar actividades de ocio saludable alternativas al uso de tecnologías de la información y comunicación
- Utilizar un lenguaje accesible y adaptado en las comunicaciones dirigidas a personas menores de edad y en la información dirigida o a la que tengan acceso personas menores de edad. Se debe evitar el uso de un lenguaje complejo o confuso, promoviendo una comunicación transparente, comprensible y accesible. Adicionalmente, se tendrá en cuenta la adaptación del lenguaje y elementos visuales a las necesidades de las personas con discapacidad y de las personas con trastorno de espectro autista.

- ***Fomento de la colaboración público-privada, la corregulación y la estandarización (artículo 11).*** Se busca impulsar que los proveedores del servicio de acceso a internet desde una ubicación fija aprueben un código de conducta que establezca los mecanismos y parámetros de configuración segura que se comprometen a aplicar en la prestación de sus servicios en lugares de acceso público en los que se presten servicios públicos y en los que se haga uso de sus servicios de acceso a internet, como escuelas, institutos, bibliotecas, centros cívicos, oficinas públicas, centros sanitarios, entre otros, para evitar el acceso a contenidos inadecuados por parte de las personas menores de edad.

- ***Estrategia nacional sobre la protección de la infancia y la adolescencia en el entorno digital (artículo 12).*** Se busca crear una Estrategia Nacional sobre la protección de la infancia y la adolescencia en el entorno digital, con carácter trianual, con el objetivo de proteger los derechos de la infancia y la adolescencia en el entorno digital. Mediante dicha estrategia se fomentará:

  - El desarrollo de actividades encaminadas a la educación en ciudadanía digital y alfabetización mediática con el fin de garantizar la plena inserción de la infancia y juventud en la sociedad digital y fomentar el uso responsable de los medios digitales que favorezca el ejercicio efectivo de sus derechos en un entorno digital seguro y respetuoso. La formación en ciudadanía digital y alfabetización mediática se abordará desde una perspectiva formativa, preventiva y social, bajo los principios de igualdad, accesibilidad, interseccionalidad, respeto, protección y garantía de los derechos de la infancia y de la adolescencia.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- La difusión de información a las madres, padres o tutores legales, equipo docente y sanitario, sobre la utilización adecuada de los dispositivos digitales y su incidencia en el desarrollo de los niños y niñas, prestando especial atención a la sensibilización sobre el ciberacoso y ciberagresiones, así como a las medidas de control parental.
- La utilización de dispositivos digitales seguros y medidas de prevención adecuadas en espacios educativos y de formación, especialmente cuando se dirijan a la infancia y juventud.
- La investigación neurobiológica, especialmente en relación con la infancia y adolescencia y los efectos de la tecnología en el desarrollo cognitivo; la investigación sobre el consumo de la pornografía y su impacto en la infancia y adolescencia; y la investigación sobre las necesidades de la infancia y adolescencia en entornos digitales.
- La creación de sistemas de aprendizaje cooperativo y de laboratorios públicos de cultura digital.

Se propone que la estrategia sea evaluada bienalmente y revisada o actualizada cada tres años teniendo en cuenta la rápida evolución tecnológica.

Finalmente, la propuesta indica las normas que quedarán derogadas y precisa las diferentes modificaciones regulatorias en diferentes sectores o ámbitos como, entre otros, los siguientes: el poder judicial, código penal, la jurisdicción contenciosa-administrativa, la ley general para la defensa de los consumidores y usuarios, la ley de protección de datos personales y garantías de los derechos digitales, la ley de comunicación audiovisual.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Desafíos a tener en cuenta al momento de crear o fortalecer las autoridades nacionales de protección de datos en los países iberoamericanos

Las principales desafíos de las autoridades de protección de datos personales pueden extraerse de algunos informes cuyos principales aspectos destacamos a continuación:

En el segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos, la Comisión Europea señaló lo siguiente:

- "Las autoridades de protección de datos requieren recursos humanos, técnicos y financieros adecuados para poder desempeñar de manera eficaz e independiente las tareas que se les encomiendan en el marco del RGPD. En el informe de 2020, la Comisión señaló que la dotación de recursos de las autoridades de protección de datos seguía sin ser satisfactoria y había planteado sistemáticamente esta cuestión a los Estados miembros. Desde entonces, la situación ha mejorado". [125]
- "Entre 2020 y 2024, en las autoridades de protección de datos, excepto en dos, se produjo un aumento del personal, y dicho aumento superó el 25 % en 14 Estados miembros.
- La autoridad de protección de datos de Irlanda registró el mayor aumento del personal (79 %), seguida de Estonia y Suecia (ambos 57 %) y Bulgaria (56 %).

[125] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 8

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Se produjo una ligera disminución del personal de la autoridad en Chequia (– 1 %), mientras que no hubo aumento en Liechtenstein y se produjeron aumentos menores en Chipre (4 %) y Hungría (8 %).
- Entre 2020 y 2024, en todas las autoridades de protección de datos, excepto en una, se produjo un aumento del presupuesto, y dicho aumento superó el 50 % en 13 Estados miembros.
- La autoridad de protección de datos de Chipre registró el mayor aumento del presupuesto (130 %), seguida de Austria (107 %), Bulgaria (100 %) y Estonia (97 %).
- El presupuesto de la autoridad griega de protección de datos disminuyó un 15 %, mientras que se produjeron pequeños aumentos presupuestarios en las autoridades de Liechtenstein (1 %), Eslovaquia (6 %) y Chequia (8 %).”[126]
-

El reporte señala que “las autoridades de protección de datos consideran que los recursos insuficientes y las lagunas en los conocimientos técnicos y jurídicos son el principal factor que afecta a su capacidad de ejecución” [127]

Las autoridades de datos, por su parte:

- “Consideran que siguen careciendo de recursos humanos suficientes. Subrayan la necesidad de conocimientos técnicos muy especializados, en particular sobre tecnologías nuevas y

[126] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 8
[127] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 6

Con el apoyo de:
Con el apoyo de:
Cooperación Española

emergentes, cuya ausencia afecta a la cantidad y la calidad de su trabajo, así como las dificultades para competir por los recursos humanos con el sector privado" [128]

- "Mencionan la insuficiencia de conocimientos jurídicos y la falta de competencias lingüísticas como factores que afectan a su desempeño" [129]
- Estiman que se afecta su capacidad de contratar y retener personal adecuado debido a la "baja remuneración, la incapacidad de seleccionar al personal de manera autónoma y la pesada carga de trabajo" [130]
- "Subrayan su necesidad de recursos financieros para modernizar y digitalizar sus procesos y adquirir equipos técnicos" [131]
- "Todas las autoridades de protección de datos desempeñan funciones que van más allá de las que les encomienda el RGPD , por ejemplo, como autoridades de control en el marco de la Directiva sobre protección de datos en el ámbito penal y la Directiva sobre la intimidad en las comunicaciones electrónicas, mientras que muchas expresan su preocupación por hacer frente a responsabilidades adicionales en virtud de la nueva legislación del ámbito digital." [132]

[128] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 8-9
[129] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 9
[130] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 9
[131] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 9
[132] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 9

PROPUESTAS

Propuesta de actualización de los estándares iberoamericanos para promover el fortalecimiento de la protección de los datos personales en el marco de las tecnologías emergentes, así como su uso ético y responsable.

La actualización de los estándares iberoamericanos de protección de datos de 2017 de la RIPDP es una necesidad urgente porque con posterioridad a su aprobación surgieron nuevos desafíos que actualmente dominan el panorama digital. La aparición de neurotecnologías capaces de leer, analizar y modificar datos del cerebro, la proliferación de sistemas de inteligencia artificial que toman decisiones automatizadas basadas en grandes volúmenes de datos, entre otros, han introducido retos no contemplados en 2017.

La evolución rápida de estas tecnologías exige que nuestros marcos de protección de datos se adapten para abordar cuestiones emergentes. Sin una actualización de los estándares de la RIPD, corremos el riesgo de que nuestra normativa sea obsoleta y no esté a la altura de las necesidades de la realidad tecnológica del siglo XXI.

Un componente fundamental de la protección efectiva de datos es el fortalecimiento de las autoridades de protección de datos. Estas instituciones deben estar equipadas con la autonomía, imparcialidad y recursos necesarios para cumplir su mandato. La capacidad de estas autoridades para llevar a cabo investigaciones, sancionar infracciones y garantizar el cumplimiento de las normativas es esencial para la protección real y efectiva de los derechos de los ciudadanos.

Particularmente preocupante y prioritario es la necesidad de proteger a los niños, niñas y adolescentes, quienes son especialmente vulnerables en el entorno digital. La exposición temprana a tecnologías que recopilan y procesan datos de manera exhaustiva pone en riesgo su privacidad y su desarrollo.

Es crucial entender que esta modernización por sí sola no producirá efectos inmediatos ni resolverá todos los desafíos asociados con la protección de datos.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Para que los nuevos estándares sean efectivos en la práctica, se deben llevar a cabo una serie de acciones adicionales indispensables:

(1) *Modificación de las normas locales:* Cada país miembro debe revisar y ajustar sus normas locales de protección de datos para alinearlas con los nuevos estándares de la RIPD. Sin una actualización normativa a nivel nacional, la implementación efectiva de los estándares regionales será limitada;

(2) *Expedir leyes de protección de datos en los países miembros de la SEGIB que aún no tienen regulación general sobre dicho tema*; (3) *Inversión en recursos:* Es necesario invertir significativamente en el fortalecimiento de las autoridades nacionales de protección de datos. Esto incluye asegurar recursos humanos, técnicos y financieros adecuados para que estas autoridades puedan desempeñar sus funciones de manera eficaz y garantizar el cumplimiento de los nuevos estándares; (4) *Diseño e implementación de políticas efectivas*: Cada país debe diseñar e implementar políticas prácticas y eficientes para asegurar que el tratamiento de datos personales y el respeto a los derechos de los individuos se lleven a cabo en la realidad. Las políticas deben ser adecuadas a las necesidades locales y estar respaldadas por una adecuada ejecución y supervisión.

Reiteramos y resumimos algunos desafíos y aspectos esenciales en torno a las autoridades de protección de datos, la neurotecnología y la inteligencia artificial y la protección de los menores en entornos digitales:

- **Autoridades de Protección de Datos**

Lo siguientes son los principales desafíos de las autoridades de protección de datos personales que pueden extraerse de un informe del Consejo de Europa del mes de julio de 2024[133]:

133 Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 8

- Recursos insuficientes: Las autoridades de protección de datos enfrentan carencia de recursos humanos, técnicos y financieros. Aunque ha habido mejoras recientes en la dotación de personal y presupuesto en algunos países, la insuficiencia de recursos sigue siendo un problema significativo.

- Conocimientos técnicos y jurídicos: La falta de conocimientos especializados en tecnologías emergentes y cuestiones jurídicas limita la capacidad de las autoridades para realizar su trabajo de manera eficaz.

- Competencia con el sector privado: Las autoridades de protección de datos tienen dificultades para atraer y retener talento debido a la baja remuneración y a la competencia con el sector privado.

- Necesidad de modernización: Existe una necesidad urgente de recursos financieros para modernizar y digitalizar procesos y adquirir equipos técnicos.

- Carga de trabajo y funciones adicionales: Las autoridades a menudo manejan funciones adicionales más allá de las establecidas por el Reglamento General de Protección de Datos (RGPD), incluyendo la supervisión bajo otras directivas y nuevas legislaciones digitales, lo que incrementa su carga de trabajo y complejidad.

- **Neurotecnologías**

Las neurotecnologías se definen como "*métodos, herramientas o dispositivos para registrar la actividad cerebral o para cambiarla*"[134]. Estas presentan importantes beneficios, como mejorar la comprensión del cerebro y desarrollar tratamientos para enfermedades neurológicas. Sin embargo, también generan riesgos significativos como, entre otros, los siguientes:

- *Usar las neurotecnologías para fines contrarios a la dignidad humana*. Con éstas se puede descodificar y alterar la actividad cerebral, lo cual genera problemas/retos éticos, jurídicos

134 Cfr. Yuste, Rafael (2024) Un paso histórico. Presentación del libro "En defensa de los neuroderechos" . Editado por la Fundación Kamanau. Pág 7

y sociales muy profundos ya que se podría cambiar la esencia del ser humano y manipularlo / alterarlo.

- *Modificar artificialmente los seres humanos*. Los hallazgos científicos en neurociencias y su aplicación a través de diversas neuro tecnologías tienen el potencial de alterar algunas características humanas fundamentales, como la autonomía, la responsabilidad moral, el libre albedrío, la dignidad, la identidad, la vida mental privada, la comprensión de los individuos como entidades atadas por sus cuerpos, la integridad y la seguridad corporal. [135]

- *Generar daños físicos al ser humano y la manipulación mental.* También pueden producir daños físicos asociados con los procedimientos invasivos de colocación de los dispositivos para mejoramiento o para la interfaz cerebro-máquina. daño tisular y deterioro de la función motora (vulneración al derecho a la integridad mental).[136]

- *Indebido tratamiento de los neurodatos y uso de los mismos para fines contrarios a la dignidad humana o no autorizados por la ley*. El "secuestro cerebral" puede implicar el robo de información (violación del derecho a la privacidad mental). También existe la posibilidad de ingreso de virus, o que los dispositivos neuronales conectados a internet posibiliten que individuos u organizaciones (hackers, corporaciones o agencias gubernamentales) rastreen o, incluso, manipulan la experiencia mental de un individuo[137].

En suma, pese a los beneficios en la salud mental que traerán las neurotecnologías, existe el temor que con la neurodata se pueda, no sólo conocer lo que piensan las personas (que por ahora es un secreto), sino manipular cerebralmente seres humanos. Por eso, desde hace poco se vienen gestando los neuroderechos que tienen como finalidad lo siguiente: (1) No perder la privacidad que tenemos respecto de nuestro cerebro (lo que pensamos); (2) Derecho a ser como soy: derecho al yo, a mi identidad cerebral natural; (3) Derecho a decidir por mí mismo, sin ser artificialmente

135 Yuste, Rafael; Goering, Sara; Bi, Guoqiang; Carmena, José M.; Carter, Adrian; Fins, Joseph J. ... & Wolpaw, Jonathan (2017). Four ethical priorities for neurotechnologies and AI. Nature News, 551 (7679), 159-163.

136 Ídem

137 Idem

manipulado o programado; (4) Neurotecnologías neutrales. No sesgadas. Que no se implanten sesgos en nuestro cerebro; y (5) Acceso equitativo a las neurotecnologías

- **Inteligencia Artificial**

En cuanto a la inteligencia artificial (en adelante IA), entendida como "un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de las entradas que recibe, cómo generar salidas tales como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después de su implementación"[138], se han destacado, entre otros, los siguientes riesgos frente al tratamiento de dato personales:

- *Sesgos:* Los datos de entrada pueden contener sesgos (datos parciales, insuficientes o desactualizados) que afectan la precisión y relevancia de los resultados.

- *Fallas Algorítmicas:* Los algoritmos pueden ser influenciados por fallas técnicas, sesgos en la lógica de programación o errores en las condiciones de operación.

- *Carencia de transparencia y Explicabilidad:* Es crucial que el tratamiento de datos mediante IA sea transparente y explicable para proteger los derechos humanos, especialmente en la toma de decisiones que afectan a las personas.

La ONU se refirió a los principios de transparencia y explicabilidad en el tratamiento de datos personales en la inteligencia artificial, mediante el Informe A/78/310 del 30 de agosto de 2023. En el informe se concluyó, entre otras, lo siguiente:

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

138 Cfr. OCDE, 2024. AI, data governance and privacy synergies and areas of international cooperation. OCDE Artificial Intelligence papers. June, no. 22. Pág 27. En: https://doi.org/10.1787/2476b1a4-en .

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 (…) porque permitirá el derecho de defensa y el debido proceso de dichas personas;

d) 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."

- **Protección de los menores de edad en entornos digitales**

El uso creciente de servicios digitales, redes sociales y aplicaciones por parte de niños, niñas y adolescentes (NNA) expone sus datos personales a diversos riesgos. Estos menores, al interactuar en plataformas digitales, a menudo comparten información personal sin comprender los peligros que esto conlleva. Datos como nombres, fotos, gustos, y correos electrónicos son fácilmente accesibles y pueden ser explotados por terceros, poniendo en riesgo su identidad digital y privacidad[139]

Es fundamental que los NNA sean conscientes de la importancia de proteger sus datos personales, ya que un uso inadecuado puede afectar su intimidad, honra y buen nombre. Los peligros a los que están expuestos incluyen ciberbullying, grooming, sexting, suplantación de identidad, y otros abusos que pueden tener un impacto negativo en su desarrollo y vida adulta. Además, la información compartida en internet contribuye a la creación de una identidad digital que afecta su presente y futuro.

139 Cfr. ONU. Informe A/HRC/46/37 del 25 de enero de 2021: La inteligencia artificial y la privacidad, así como la privacidad de los niños - Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci. Pág. 22 .

Progresivamente han aumentado los casos que evidencian los riesgos y peligros a los que se ven expuestos los NNA en las redes sociales digitales. Se ha puesto de presente que *"Los niños, niñas y adolescentes tienen cada vez mayor acceso a los distintos sistemas de comunicación, que les permiten obtener todos los beneficios que ellos representan, pero esta situación también ha llevado al límite el balance entre el ejercicio de los derechos fundamentales y los riesgos —para la vida privada, el honor, buen nombre, y la intimidad, entre otros— que, así como los abusos de los cuales pueden ser víctimas —como discriminación, explotación sexual, pornografía, entre otros— pueden tener un impacto negativo en su desarrollo integral y vida adulta"*[140]

Es muy importante no perder de vista lo anterior, pues, a partir de la información que existen sobre NNA en internet o redes sociales digitales se crea la identidad digital de aquellos, la cual incide en su presente y futuro como seres humanos.

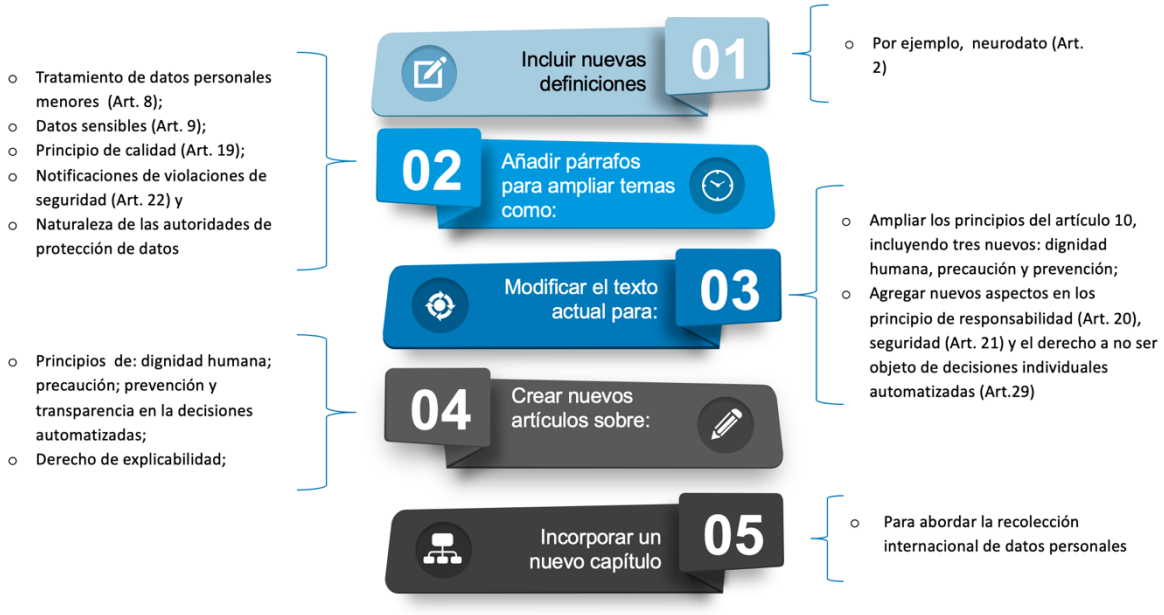
¿En qué consisten las modificaciones?

Teniendo en cuenta algunos de los desafíos enunciados en este documento se sugiere, realizar varios cambios a los Estándares de la RIPD de 2017, los cuales resumimos en esta gráfica:

140 Memorandum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes -(2009).

Con el apoyo de:
Con el apoyo de:
Cooperación Española

ASPECTOS GENERALES DE LA PROPUESTA DE ACTUALIZACIÓN DE LOS ESTÁNDARES DE LA RIPD DE 2017



Resumen de las propuestas de actualización de los estándares de la RIPD de 2017

- Incluir nuevas definiciones como, por ejemplo, neurodato (Art. 2)
- Adicionar párrafos para complementar algunos temas relevantes. Esto se hace respecto de los siguientes:
    - Tratamiento de datos personales de niñas, niños y adolescentes (Art. 8);
    - Tratamiento de datos personales de carácter sensible (Art. 9);
    - Principio de calidad (Art. 19);
    - Notificaciones de vulneraciones a la seguridad de los datos personales (Art. 22) y
    - Naturaleza de las autoridades de control y supervisión
- Modificar partes del texto actual. Por ejemplo:
    - (i) se amplía los principios del artículo 10, incluyendo tres nuevos, a saber: dignidad humana, precaución y prevención;

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- (ii) se incluyen nuevos aspectos en los principios de responsabilidad (Art. 20), seguridad (Art. 21) y el derecho a no ser objeto de decisiones individuales automatizadas (Art.29). En este último, se adiciona un parágrafo con algunas prohibiciones sobre prácticas relacionadas con el tratamiento de datos y la IA en línea de lo señalado en el artículo 5 del REIA .
-

- Incorporar artículos nuevos que tratan los siguientes temas:
  - Principio de dignidad humana;
  - principio de precaución;
  - principio de prevención;
  - transparencia en las decisiones automatizadas;
  - derecho de explicabilidad;
- Crear un nuevo capítulo sobre recolección internacional de datos personales

A continuación nos referiremos a los aspectos específicos de la propuesta

Propuestas sobre Autoridades de Protección de Datos (APD)

Teniendo en cuenta la información sobre los desafíos que enfrentan las autoridades de protección de datos, sugerimos lo siguiente para fortalecer a las autoridades de protección de datos en los países miembros de la SEGIB[141]:

[141] Teniendo en cuenta lo señalado sobre las autoridades de datos, sugerimos a la SEGIB acoger las siguientes recomendaciones de la Comisión Europea incorporadas en el informe publicado el 25 de julio de 2024.

Los Estados miembros de la SEGIB deberán:

"- garantizar la independencia plena y efectiva de las autoridades nacionales de protección de datos;

"- asignar recursos suficientes a las autoridades de protección de datos para que puedan desempeñar sus funciones, en particular mediante la provisión de los recursos técnicos y los

1. *Asegurar la autonomía e independencia de las APD*: Es fundamental que las autoridades puedan tomar decisiones imparciales y actuar sin la influencia de factores externos. Esto implica también eliminar cualquier tipo de presión política o económica que pudiera interferir con el cumplimiento de sus funciones.

2. *Dotar de recursos suficientes a las APD:* Es urgente garantizar la dotación adecuada de recursos humanos, técnicos y financieros. Sin estos recursos, las autoridades no podrán cumplir con sus funciones de manera efectiva. Se recomienda aumentar el presupuesto dedicado a estas autoridades, asegurando que cuenten con el personal capacitado y el equipo tecnológico necesario para enfrentar los desafíos derivados del crecimiento del entorno digital.

3. *Capacitar técnica y jurídicamente al equipo humano de las APD:* La rápida evolución de las tecnologías emergentes exige que el personal de las autoridades de protección de datos tenga conocimientos especializados. Se deben implementar programas de capacitación continua para que los equipos de estas autoridades puedan responder eficazmente a los retos tecnológicos y jurídicos que enfrentan.

---

conocimientos especializados necesarios para hacer frente a las tecnologías emergentes y cumplir nuevas responsabilidades en virtud de la legislación digital;

"- dotar a las autoridades de protección de datos de los instrumentos de investigación necesarios para que puedan utilizar eficazmente los poderes de ejecución (…);

"- apoyar el diálogo entre las autoridades de protección de datos y otros reguladores nacionales, en particular aquellos que se creen en virtud de nuevos instrumentos jurídicos en materia digital.

"- garantizar que se consulte oportunamente a las autoridades de protección de datos antes de la adopción de la legislación sobre el tratamiento de datos personales." (CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 33)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

4. *Modernizar las infraestructuras de las APD:* Esto incluye la digitalización de sus procesos y la adquisición de tecnologías avanzadas que faciliten su gestión.

5. *Revisar los esquemas de remuneración de los empleados de las APD:* Las autoridades enfrentan competencia con el sector privado para atraer y retener talento especializado, debido a las diferencias salariales. Por ende, se recomienda crear incentivos económicos y oportunidades de desarrollo profesional para evitar la fuga de talento.

Finalmente, y en cuanto al texto de los estándares de la RIPD, se sugiere adicionar al artículo 42 dos numerales para que las APD: (1) Creen mecanismos de especial atención para la población vulnerable como, entre otros, los menores, y (2) Promuevan el uso del alternativas de solución de controversias sobre tratamiento de datos personales que contribuyan a la protección mas eficiente, efectiva y expedita de los derechos de las personas.

Propuestas sobre Neurotecnologías

Respecto de las neurotecnologías se sugiere lo siguiente en los estándares:

(1) Incluir la definición de neurodato y catalogarlo como un dato sensible que debe ser objeto de medidas especiales de responsabilidad reforzada de manera que exista mayor seguridad, confidencialidad, acceso y circulación restringida para evitar su conocimiento o uso indebido así como su manipulación o destrucción;

(2) Señalar que en el tratamiento de datos neuronales o neurodatos no se podrá manipular o alterar la libertad de pensamiento y conciencia, haciendo que el individuo 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, rehabilitación y 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.

(3) Adicionar los siguienteres principios:

(3.1) **Dignidad humana** para que los Estados adopten medidas necesarias y eficaces, incluso de orden legislativo, para impedir que el tratamiento de datos personales y los logros científicos o tecnológicos se utilicen en detrimento de la dignidad humana, los derechos humanos, las libertades fundamentales, la sociedad y la humanidad;

(3.2) **Precaución** para que, en caso de presentarse falta de certeza frente a los potenciales daños al titular del dato o la sociedad con ocasión del tratamiento de datos personales, y con miras a evitar que se cause un daño grave e irreversible, el Responsable o Encargado del tratamiento se abstengan de realizar dicho tratamiento o adoptar medidas precautorias o preventivas para proteger los derechos del titular del dato, su dignidad humana y otros derechos humanos; y

(3.3.) **Prevención** para que los Responsables y Encargados del tratamiento de datos personales implementen medidas para evitar daños o perjuicios a los titulares de los datos, o vulnerar sus derechos.

En adición a lo anterior, se recomienda lo siguiente:

(4) Apoyar la propuesta de la UNESCO para crear y adoptar una regulación global sobre la ética de la neurotecnología. Los Estados Miembros aprobaron la puesta en marcha de esta iniciativa durante la reunión número 42 de la Conferencia General de la UNESCO, en noviembre de 2023.

(5) Promover la expedición de una ley modelo sobre los principios en materia de neurociencias, neurotecnologías y derechos humanos. Como punto de partida, se recomienda tener presente, entre otros, los siguientes documentos: a) "Declaración de principios interamericanos en materia de neurociencias, neurotecnologías y derechos humanos", aprobada en marzo de 2023 por el Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA), (b) la Declaración sobre neurotecnologías y neurodatos de la EIPD en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29

de mayo de 2024); (c) La Declaración de la RIPD sobre neurodatos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en la Antigua, Guatemala el 25 de septiembre de 2023, y (d) La Ley Modelo de Neuroderechos para América Latina y el Caribe aprobada por la Parlamento Latinoamericano y Caribeño.

Propuestas sobre Inteligencia Artificial

En cuanto a la inteligencia artificial, se recomienda lo siguiente en los estándares:

(1) En en principio de calidad señalar que, de una parte, los datos personales deberán ser veraces, comprobables y pertinentes respecto de la finalidad del tratamiento. Y, de otra parte, prohibir el tratamiento de datos que genere o induzcan a error respecto de las decisiones que se tomen sobre los seres humanos.

(2) Incluir un artículo sobre transparencia en las decisiones automatizadas, en la elaboración de perfiles o procesos de decisión mediante inteligencia artificial u otras tecnologías.

(3) Crear el derecho de explicabilidad para que, cuando lo solicite el titular del dato, el Responsable o Encargado le proporcione explicaciones en un lenguaje claro y comprensible respecto de la información y el proceso realizado para adoptar una decisión que afecta a dicha persona.

(4) Incluir algunas prohibiciones sobre prácticas relacionadas con el tratamiento de datos en línea con lo señalado en el artículo 5 del REIA.

Propuestas sobre protección de los menores de edad en entornos digitales

En cuanto a la protección de los menores, se recomienda lo siguiente en los estándares:

(1) Señalar expresamente que el tratamiento de datos personales de menores debe ser objeto de medidas especiales de responsabilidad reforzada de manera que existan

Con el apoyo de:
Con el apoyo de:
Cooperación Española

mayores medidas de seguridad, confidencialidad, acceso y circulación restringida para evitar su acceso o uso indebido así como su manipulación o destrucción.

Texto de las modificaciones sugeridas

Para la redacción de la propuesta se tuvieron en cuenta, entre otros, los siguientes documentos:

- GPA (Global Privacy Assembly), 2023. Resolución "Alcanzando estándares globales de protección de datos: principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo" [142]
- ONU, Informe A/79/173 del 17 de julio de 2024 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 computarizados de datos personales". [143] Propuesta de actualización de la ONU (2024)
- Propuesta de una Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales (2024) publicada en el siguiente libro: Transferencia internacional de dados pessoais na América Latina. Rumo a harmonizacao de normas[144].

[142] Cfr. Global Privacy Assembly (GPA). 45th Closed Session of the Global Privacy Assembly. October 2023. Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. En: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

[143] El texto de la propuesta contenida en el informe A/79/173 del 17 de julio de 2024 fue presentado por Ana Brian, Relatora Especial de la ONU sobre el derecho a la privacidad, puede consultarse en: https://www.ohchr.org/es/documents/thematic-reports/a79173-report-special-rapporteur-right-privacy-ana-brian-nougreres . El autor de este estudio fue parte del equipo que colaboró en la redacción del informe y de la propuesta.

[144] Cfr. Belli, Luca; Brian, Ana; Mendoza, Jonatha; Palazzi, Pablo y Remolina, Nelson. (2024) Transferencia internacional de dados pessoais na América Latina. Rumo a harmonizacao de normas. Lumen Juris editora y Fundación Getulio Vargas. Rio de Janeiro, Brasil. ISBN: 978-85-519-

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 2. Definiciones

Incluir esta nueva definición.

- **Neurodato**: es todo dato que se obtiene del sistema nervioso central y periférico de una persona mediante el uso de neurotecnologías. Estos datos ultrasensibles pueden permitir la identificación personal, o revelar información sobre el estado o condiciones de salud en los distintos momentos del ciclo vital, y en los diferentes procesos de salud.

Adicionar los "neurodatos" como otro ejemplo de datos personales sensibles (literal -d- del numeral 2.1.). El texto quedaría así:

"d. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos, los neurodatos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Artículo 8. Tratamiento de datos personales de niñas, niños y adolescentes

Adicionar el siguiente numeral:

8.3. El tratamiento de datos personales de niñas, niños y adolescentes deberá ser objeto de medidas especiales de responsabilidad reforzada de manera que existan mayores medidas de seguridad,

3246-9. El texto está disponible en: https://repositorio.fgv.br/items/98aaa2e4-7279-4649-8dae-836ca8a65bae

confidencialidad, acceso y circulación restringida para evitar su acceso o uso indebido así como su manipulación o destrucción.

Artículo 9. Tratamiento de datos personales de carácter sensible.

Adicionar estos dos numerales:

9.3. En el tratamiento de datos neuronales o neurodatos no se podrá manipular o alterar la libertad de pensamiento y conciencia, haciendo que el individuo 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, rehabilitación y 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.

9.4. El tratamiento de datos personales sensibles deberá ser objeto de medidas especiales de responsabilidad reforzada de manera que existan mayores medidas de seguridad, confidencialidad, acceso y circulación restringida para evitar su acceso o uso indebido así como su manipulación o destrucción.

Artículo 10. Principios aplicables al tratamiento de datos personales

Realizar la siguiente modificación.

10.1. En el tratamiento de datos personales, el responsable observará los principios de dignidad humana, precaución, prevención, legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Artículo nuevo. Principio de dignidad humana

Los Estados adoptarán medidas necesarias y eficaces, incluso de orden legislativo, para impedir que el tratamiento de datos personales y los logros científicos o tecnológicos se utilicen en detrimento de la dignidad humana, los derechos humanos, las libertades fundamentales, la sociedad y la humanidad.

Artículo nuevo. Principio de precaución

En caso de presentarse falta de certeza frente a los potenciales daños al titular del dato o la sociedad con ocasión del tratamiento de datos personales, y con miras a evitar que se cause un daño grave e irreversible, el Responsable o Encargado del tratamiento deberán abstenerse de realizar dicho tratamiento o adoptar medidas precautorias o preventivas para proteger los derechos del titular del dato, su dignidad humana y otros derechos humanos.

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

Artículo nuevo. Principio de prevención

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Los Responsables y Encargados del tratamiento de datos personales deberán implementar medidas preventivas para evitar daños o perjuicios a los titulares de los datos, o vulnerar sus derechos.

Artículo 19. Principio de calidad

Adicionar el siguiente párrafo al numeral 19.1 (Principio de calidad):

19.1. El responsable adoptará las medidas necesarias para mantener exactos, completos

y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

"Los datos personales deberán ser veraces, comprobables y pertinentes respecto de la finalidad del tratamiento. No deberá permitirse el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error."

Artículo 20. Principio de responsabilidad

Efectuar el siguiente ajuste al numeral 20.1 (Principio de responsabilidad)

20.1. El responsable implementará mecanismos útiles, pertinentes, eficaces y oportunos que necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Artículo 21. Principio de seguridad

Realizar el siguiente ajuste al numeral 21.1 (Principio de seguridad)

21.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento

que efectúe, medidas de carácter administrativo, humano, contractual, físico, técnico y de cualquier otra naturaleza que sean suficientes para , de una parte, garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos personales y, de otra parte, evitar la pérdida, manipulación, consulta, uso o acceso no autorizado o fraudulento de dicha información.

En el caso de datos personales sensibles y de niñas, niños o adolescentes, implementará medidas más estrictas para garantizar la seguridad y confidencialidad de la información (seguridad reforzada).

.

Artículo 22. Notificación de vulneraciones a la seguridad de los datos personales

Adicionar el siguiente párrafo al numeral 22.1

“Adicionalmente, deberá adoptar las medidas necesarias para evitar que cualquier incidente de seguridad cause daño a los titulares de los datos, o que, según el caso, el mismo sea el mínimo posible.”

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 29. Derecho a no ser objeto de decisiones individuales automatizadas

Adicionar lo siguiente en el artículo 29.4.

29.4. El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos, neurodatos o datos biométricos.

Parágrafo: No se podrá realizar tratamiento de datos personales que con el objeto o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

Adicionalmente, prohíbe el tratamiento de datos que:

- Explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra; [145]
- Evalúe o clasifique a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes: i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente; ii) un trato perjudicial o desfavorable hacia

[145] Cfr. Literal b) del artículo 5 del REIA

Con el apoyo de:
Con el apoyo de:
Cooperación Española

determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este; [146]

- Realice evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad;[147]
- Cree o amplíe bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;[148]
- Infiriera las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el tratamiento esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad; [149]
- Clasifique individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; [150]
- Realice identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso cumpla unos requisitos y sea estrictamente necesario para alcanzar uno o varios objetivos relacionados con la búsqueda de víctimas de algunos delitos, la prevención de atentados terroristas o la captura de personas sospechosas de haber cometido un delito. [151]

---

[146] Cfr. Literal c) del artículo 5 del REIA

[147] Cfr. Literal d) del artículo 5 del REIA. "Esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva"

[148] Cfr. Literal e) del artículo 5 del REIA

[149] Cfr. Literal f) del artículo 5 del REIA

[150] Cfr. Literal g) del artículo 5 del REIA. "Esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho"

[151] Cfr. Literal h) del artículo 5 del REIA.Los objetivos permitidos son los siguientes:" i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas, ii) la prevención de una amenaza

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo nuevo. Transparencia en las decisiones automatizadas

En el caso de que el titular del dato esté sometido a decisiones automatizadas, en la elaboración de perfiles o procesos de decisión mediante inteligencia artificial u otras tecnologías se le deberá informar de manera clara y sencilla al titular del dato lo siguiente:

- Que en el tratamiento de sus datos personales se utilizarán procesos de automatización, inteligencia artificial o cualquier otra tecnología.
- Información clara, veraz y significativa sobre la lógica aplicada para tomar una decisión que afecta a un ser humano 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.
- Suministrar información adicional que le permita al titular del dato conocer la forma cómo las decisiones automatizadas pueden afectarlos positiva o negativamente. La información se debe suministrar en un lenguaje claro, sencillo y de fácil comprensión.
- Darle a conocer que tiene el derecho de explicabilidad

Artículo nuevo. Derecho de explicabilidad

específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista, iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos que tengan como sanción una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años."

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Cuando lo solicite el titular del dato, 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 debe 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 los afectan y para para que puedan tener herramientas para defender sus derechos humanos o solicitar la revisión de la decisión.

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

Crear un capítulo nuevo titulado Recolección internacional de datos personales

Luego del capítulo V sobre transferencias internacionales de datos (artículos 36), crear este capítulo con el siguiente contenido.

Artículo nuevo. Recolección internacional de datos. 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 es recolectada desde terceros países por parte de responsables o encargados ubicados en países diferentes al del domicilio o residencia del titular del dato personal y que no tienen sede física o establecimiento en el mismo (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.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

La no presencia, residencia física o establecimiento del recolector internacional de datos en el país del titular del dato no debe generar o facilitar impunidad o falta de protección de los derechos de las personas.

Artículo 42. Naturaleza de las autoridades de control y supervisión

Crear los siguientes numerales:

42.7. Las autoridades de control deberán crear mecanismos de especial atención para la población vulnerable como, entre otros, los niños, las niñas y los adolescentes.

42.8. En adición a las acciones judiciales o administrativas previstas en la regulación nacional, las autoridades de control promoverán el uso del alternativas de solución de controversias sobre tratamiento de datos personales que contribuyan a la protección mas eficiente, efectiva y expedita de los derechos de las personas.

Propuesta para proteger los niños, las niñas y los adolescentes frente a los desafíos de la sociedad digital.

Expedir regulación que de manera integral busque proteger los niños, las niñas y los adolescentes frente a los desafíos de la sociedad digital. Se recomienda tomar como referencia la propuesta de España de junio de 2024 contemplada en el anteproyecto de ley orgánica para la protección de las personas menores de edad en los entornos digitales. Como se mencionó, esta iniciativa es un propuesta de regulación holistica que comprende medidas en diferentes ámbitos (la protección de los consumidores y usuarios; educativo; sanitario y el sector público) para proteger a las personas menores de edad en el mencionado entorno.

La propuesta reconoce los beneficios de los medios tecnológicos para la sociedad, pero destaca algunos riesgos que es necesario mitigar. En concreto, plantea que “el uso inadecuado de estos

Con el apoyo de:
Con el apoyo de:
Cooperación Española

medios digitales, por las personas menores de edad, o por los adultos en relación con ellos, puede provocar importantes perjuicios a los menores y a sus familias, tales como daños psicológicos y emocionales; daños para la salud física; desinformación, manipulación y construcción de falsas creencias; establecimiento de conductas peligrosas o socialmente inapropiadas; inclusión en grupos y colectivos dañinos; adicciones; o perjuicios económicos."[152]

Dado lo anterior, el proyecto de ley tienes estas finalidades: (1) "Garantizar el respeto y cumplimiento de los derechos de las niñas, niños y adolescentes en el entorno digital, especialmente los derechos a la intimidad, al honor y a la propia imagen, al secreto de las comunicaciones y a la protección de los datos personales y el acceso a contenidos adecuados a la edad; (2) "Fomentar un uso equilibrado y responsable de los entornos digitales a fin de garantizar el adecuado desarrollo de la personalidad de las personas menores de edad y de preservar su dignidad y sus derechos fundamentales; (3) "Garantizar que los productos y servicios digitales tengan en cuenta, desde su diseño y por defecto, el interés superior del menor; (4) "Apoyar el desarrollo de las competencias digitales de la infancia en el entorno digital y la capacidad de evaluar los contenidos en línea y detectar la desinformación y el material abusivo; (5) "Promover un entorno digital más seguro y estimular la investigación en este ámbito." [153]

Adicionalmente, la propuesta incluye los siguientes derechos para los menores de edad: (1) "Ser protegidas eficazmente ante contenidos digitales que puedan perjudicar su desarrollo.; (2) "Recibir información suficiente y necesaria en una forma y lenguaje apropiado según la edad sobre el uso de las tecnologías, así como de sus derechos y de los riesgos asociados al entorno digital; (3) "Acceso a la información, a la libertad de expresión, y a ser escuchadas; (4) "Acceso equitativo y efectivo a dispositivos, conexión y formación para el uso de herramientas digitales." [154]

152 Ídem

153 Cfr. Artículo 2 del ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES.

154 Cfr. Artículo 2 del ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES.

El proyecto se divide en varios títulos, cuyo contenido esencial enunciamos a continuación :

Título I. Medidas en el ámbito de la protección de los consumidores y usuarios: Obligaciones de los fabricantes de dispositivos digitales con conexión a internet; Regulación del acceso y activación de los mecanismos aleatorios de recompensa.

Título II. Medidas en el ámbito educativo: Actividades de formación en los centros de educación infantil, primaria, secundaria obligatoria y secundaria postobligatoria; Regulación del uso de dispositivos en los centros de educación infantil, primaria, secundaria obligatoria y secundaria postobligatoria.

Título III. Medidas en el ámbito sanitario: Prevención y promoción de la salud; Atención especializada.

Título IV. Medidas en el sector público: Participación, información y sensibilización; Fomento de la colaboración público-privada, la corregulación y la estandarización; Estrategia nacional sobre la protección de la infancia y la adolescencia en el entorno digital .

A continuación se ilustran los aspectos generales de la propuesta:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

PROPUESTA PARA PROTEGER LOS NIÑOS, LAS NIÑAS Y LOS ADOLESCENTES FRENTE A LOS DESAFÍOS DE LA SOCIEDAD DIGITAL.

Establecer medidas con la finalidad de garantizar la protección de las personas menores de edad en los entornos digitales

Fuente. ANTEPROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES, elaborada por los siguientes ministerios de España: Ministerio de la presidencia, justicia y relaciones con las cortes ; Ministerio de juventud e infancia; Ministerio para la transformación digital y de la función pública, y Ministerio de derechos sociales, consumo y agenda 2030.

Propuesta respecto de neurotecnologías

Teniendo en cuenta los desafíos sobre el tema, se sugiere, entre otras, lo siguiente a los Jefes de Estado de los países miembros de la SEGIB:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Promover la expedición de una ley que regule los principios en materia de neurociencias, neurotecnologías y derechos humanos. Se sugiere que el contenido de la regulación incluya el siguiente modelo o esquema en su estructura:

Artículo 1. Objeto y ámbito de aplicación.

Artículo 2. Definiciones.

Artículo 3. Dignidad humana

Artículo 4. Identidad, autonomía, privacidad de la actividad neuronal y manipulación cerebral

Artículo 5. Ética y protección de los Derechos Humanos desde el diseño y por defecto de las neurotecnologías.

Artículo 6. Principio de precaución

Artículo 7. Los datos neuronales como datos personales altamente sensibles.

Artículo 8. Responsabilidad demostrada y seguridad en el tratamiento de neurodatos

Artículo 9. Consentimiento expreso e informado para el tratamiento de los neurodatos

Artículo 10. Igualdad, no Discriminación y acceso equitativo a las neurotecnologías.

Artículo 11. Aplicación terapéutica exclusiva respecto al aumento de las capacidades cognitivas.

Artículo 12. Integridad neurocognitiva

Artículo 13. Gobernanza transparente de las neurotecnologías.

Artículo 14. Supervisión y fiscalización de las neurotecnologías.

Artículo 15. Protección efectiva de los derechos.

Artículo 16. Solidaridad , cooperación y beneficios compartidos.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 17. Protección de las generaciones futuras.

Artículo 18. Gratuidad y no comercialización.

Artículo 19. Transferencia de tecnología y conocimientos.

Se anexa una propuesta de ley modelo (ver anexo 1), respecto de la cual se precisa lo siguiente:

La propuesta incorpora (con pequeñas modificaciones) el contenido de la "Declaración de principios interamericanos en materia de neurociencias, neurotecnologías y derechos humanos", aprobada por el Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA)[155] y, de otra, adiciona otros principios sobre: a) tratamiento de datos personales, y b) investigación y uso de las tecnologías biomédicas.

También incorpora lineamientos y directrices de los siguientes documentos:

Red Iberoamericana de protección de datos (RIPD)

- RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024).

[155] Cfr. Organización de Estados Americano (OEA). Comité Jurídico Interamericano. *Declaración de principios interamericanos en materia de neurociencias, neurotecnologías y derechos humanos.* 102 PERÍODO ORDINARIO DE SESIONES OEA/Ser. Q. 6 – 10 de marzo, 2023 CJI/RES. 281 (CII-O/23) corr.1. Rio de Janeiro, Brasil 9 marzo 2023

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- RIPD, 2023. Declaración sobre neurodatos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en la Antigua, Guatemala el 25 de septiembre de 2023.
- RIPD, 2017. Estándares de protección de datos personales para los países Iberoamericanos

Organización de Estados Americanos (OEA)

- OEA, 2023. Declaración de principios interamericanos en materia de neurociencias, neurotecnologías y derechos humanos. Aprobada en marzo de 2023 por el Comité Jurídico Interamericano de la Organización de Estados Americanos
- OEA, 2021. Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones expedidos el 9 de abril de 2021 por el Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA). Estos principios fueron aprobados por la Asamblea General de la OEA en noviembre de 2021.
- OEA, 2021. Declaración sobre neurociencia, neurotecnologías y derechos humanos: nuevos desafíos jurídicos para las américas. Aprobada en agosto de 2021 por el Comité Jurídico Interamericano de la Organización de Estados Americanos-

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)

- UNESCO, 2005. Declaración universal sobre bioética y derechos humanos. Aprobada por aclamación por la 33a sesión de la Conferencia General de la UNESCO, el 19 de octubre de 2005. En: https://unesdoc.unesco.org/ark:/48223/pf0000146180_spa
- UNESCO, 2003. Declaración internacional sobre los datos genéticos humanos. Aprobada por aclamación por la 29 sesión de la Conferencia General de la UNESCO, el 16 de octubre de 2003. En: https://unesdoc.unesco.org/ark:/48223/pf0000253908_spa
- UNESCO, 1997. Declaración universal sobre el genoma y los derechos humanos. Aprobada por aclamación por la 29 sesión de la Conferencia General de la UNESCO, el 11 de noviembre de 1997. En: https://unesdoc.unesco.org/ark:/48223/pf0000253908_spa

Parlamento Latinoamericano y Caribeño (PLC)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- PLC, 2023. Ley Modelo de Neuroderechos para América Latina y el Caribe (Panamá 19 y 20 de mayo 2023)

Es importante señalar que existen declaraciones internacionales cuyo contenido puede replicarse al campo de las neuro tecnologías. Dentro de ellas, destacamos las siguientes:

Declaración Universal sobre bioética y derechos humanos de la UNESCO[156]

La citada Declaración trata "las cuestiones éticas relacionadas con la medicina, las ciencias de la vida y las tecnologías conexas aplicadas a los seres humanos, teniendo en cuenta sus dimensiones sociales, jurídicas y ambientales" y enuncia una serie de principios y procedimientos que le permita a los Estados formular regulación y políticas relacionadas con la bioética en el ámbito de la investigación científica así como el acceso a los beneficios científicos generados.

Estos son los principios orientadores:

- Dignidad y derechos humanos
- Beneficios y efectos nocivos
- Autonomía y responsabilidad individual
- Consentimiento
- Protección de personas carentes de la capacidad de dar su consentimiento
- Respeto de la vulnerabilidad humana y la integridad personal

[156] UNESCO, 2005. Declaración universal sobre bioética y derechos humanos. Aprobada por aclamación por la 33a sesión de la Conferencia General de la UNESCO, el 19 de octubre de 2005. En: https://unesdoc.unesco.org/ark:/48223/pf0000146180_spa

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Privacidad y confidencialidad
- Igualdad, justicia y equidad
- No discriminación y no estigmatización
- Respeto de la diversidad cultural y del pluralismo
- Solidaridad y cooperación
- Responsabilidad social y salud
- Aprovechamiento compartido de los beneficios
- Protección de las generaciones futuras,
- Protección del medio ambiente, la biosfera y la biodiversidad

Declaración universal sobre el genoma humano y los derechos humanos de la UNESCO.[157]

En la Declaración se establece lo siguiente que, por su importancia, se trascribe porque puede replicarse para la investigación en neurociencias y el uso de neurotecnologías:

- "Una investigación, un tratamiento o un diagnóstico en relación con el genoma de un individuo, sólo podrá efectuarse previa evaluación rigurosa de los riesgos y las ventajas que entraña y de conformidad con cualquier otra exigencia de la legislación nacional" (Literal a) del artículo 5)
- "Ninguna investigación relativa al genoma humano ni sus aplicaciones, en particular en las esferas de la biología, la genética y la medicina, podrán prevalecer sobre el respeto de los derechos humanos, de la libertades fundamentales y de la dignidad humana de los individuos o, si procede, de los grupos humanos" (Artículo 10)
- "No deben permitirse las prácticas que sean contrarias a la dignidad humana, como la clonación con fines de reproducción de seres humanos." (Artículo 11)

[157] UNESCO, 1997. Declaración universal sobre el genoma humano y los derechos humanos. Aprobada por aclamación por la 29 sesión de la Conferencia General de la UNESCO, el 11 de noviembre de 1997. En: https://unesdoc.unesco.org/ark:/48223/pf0000253908_spa

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- "Toda persona debe tener acceso a los progresos de la biología, la genética y la medicina en materia de genoma humano, respetándose su dignidad y derechos" (Literal a) del artículo 12)
- "Las aplicaciones de la investigación sobre el genoma humano, en particular en el campo de la biología, la genética y la medicina, deben orientarse a aliviar el sufrimiento y mejorar la salud del individuo y de toda la humanidad" (Literal b) del artículo 12)
- "Las consecuencias éticas y sociales de las investigaciones sobre el genoma humano imponen a los investigadores responsabilidades especiales de rigor, prudencia, probidad intelectual e integridad, tanto en la realización de sus investigaciones como en la presentación y explotación de los resultados de éstas. Los responsables de la formulación de políticas científicas públicas y privadas tienen también responsabilidades especiales al respecto." (Artículo 13)
- "Los Estados tomarán las medidas apropiadas para fijar el marco del libre ejercicio de las actividades de investigación sobre el genoma humano respetando los principios establecidos en la presente Declaración, a fin de garantizar el respeto de los derechos humanos, las libertades fundamentales y la dignidad humana y proteger la salud pública. Velarán por los resultados de esas investigaciones no puedan utilizarse con fines no pacíficos." (Artículo 15)
- "Los Estados reconocerán el interés de promover, en los distintos niveles apropiados, la creación de comités de ética independientes, pluridisciplinarios y pluralistas, encargados de apreciar las cuestiones éticas, jurídicas y sociales planteadas por las investigaciones sobre el genoma humano y sus aplicaciones" (Artículo 16)

ANEXOS

Anexo 1 : Propuesta de ley modelo mediante la cual se regulan principios en materia de neurociencias, neurotecnologías y derechos humanos

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Propuesta de ley modelo mediante la cual se regulan principios en materia de neurociencias, neurotecnologías y derechos humanos[158]

Artículo 1. Objeto y ámbito de aplicación.

La presente ley tiene por objeto definir y adoptar los principios que deben orientar la investigación y aplicación de las neurociencias y las neurotecnologías con el fin de garantizar la protección de la dignidad humana y los derechos humanos, dentro del marco de la innovación tecnológica y los desarrollos científicos.

Los principios y disposiciones contenidas en la presente ley son vinculantes y aplicables a las entidades públicas o privadas, y en general a cualquier persona natural o jurídica, que realice tratamiento de neurodatos o diseñe, desarrolle o use neurotecnologías. Para garantizar el cumplimiento de los mismos deberán elaborar un plan de acción progresivo que dé cuenta de la adopción, incorporación y aplicación de los mismos en procura de la protección de los derechos humanos.

En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los principios y disposiciones de la misma.

[158] Esta propuesta es fruto del trabajo interdisciplinario de las siguientes universidades colombianas: Facultades de Derecho de la Universidad de los Andes, Facultad de Medicina de la Universidad del Rosario y la Facultad de Jurisprudencia de la Universidad del Rosario . En la redacción participaron los (as) profesores (as) Nelson Remolina Angarita (Universidad de los Andes), Ana Isabel Gómez Córdoba y Diana Rocío Bernal Camargo (Universidad del Rosario) y Carlos Julio González, Senador de la República de Colombia.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 2. Definiciones.

Para los efectos de la presente ley, se entiende por:

- **Consentimiento informado:** Es la manifestación de voluntad libre, previa, específica, expresa e informada de la persona para el uso de neurotecnologías en distintos ámbitos así como para el tratamiento de los neurodatos después de haber recibido información sobre los objetivos, fines, riesgos y beneficios asociados.

- **Continuidad psicológica:** es una cadena, que se extiende en el tiempo y está en permanente evolución, de los recuerdos, creencias, deseos, rasgos de personalidad y experiencias, que constituyen la identidad de una persona.

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

- **Dato personal sensible**: Es aquella información que afecta la intimidad del Titular 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, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;

- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- **Neurociencias**: Son el estudio interdisciplinar del sistema nervioso.

- **Neurodato**: es todo dato que se obtiene del sistema nervioso central y periférico de una persona mediante el uso de neurotecnologías. Estos datos ultrasensibles pueden permitir la identificación personal, o revelar información sobre el estado o condiciones de salud en los distintos momentos del ciclo vital, y en los diferentes procesos de salud.

- **Neuroderechos**: son una categoría de derechos humanos emergentes que buscan garantizar la dignidad y los derechos fundamentales en el ámbito de la investigación y el uso de las neurociencias y las neurotecnologías.

- **Neurotecnologías**: son cualquier tecnología que registre, intérprete, altere o interfiera con la actividad cerebral, mediante diversas técnicas ópticas, electrónicas, magnéticas y nanotecnológicas, que permiten comprender los procesos cerebrales, como la visión, las sensaciones, las percepciones, el comportamiento, las ideas, la memoria, las emociones, la conciencia, la imaginación, las decisiones y la mente. Permiten detectar la correlación entre los estados mentales y el comportamiento

- **Neurotecnologías invasivas:** técnicas que registran o alteran la actividad cerebral desde el interior del cerebro, lo que implica procedimientos médicos intrusivos en el cuerpo humano.

- **Neurotecnologías no invasivas:** técnicas que registran la actividad del cerebro o alteran la actividad cerebral desde el exterior del cráneo.

- **Titular del dato**: Persona natural cuyos datos personales sean objeto de Tratamiento

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 3. Dignidad humana.

La dignidad como valor supremo inherente al ser humano es inviolable.

El Estado promoverá un enfoque basado en el respeto a la dignidad humana y los derechos humanos en el diseño, desarrollo, implementación, comercialización, evaluación y uso de las neurotecnologías.

La dignidad humana también comprende la dignidad póstuma, lo cual significa que el cadáver y sus componentes deben ser objeto de consideración moral y ética. Los neurodatos están íntimamente ligados con la identidad de la persona y pueden persistir después de la muerte. Esto obliga a que se garantice la dignidad póstuma en el tratamiento de los neurodatos después del fallecimiento, lo que implica que solo puedan ser usados según los deseos previamente expresados por la persona según sus valores, creencias y preferencias.

Artículo 4. Identidad, autonomía, privacidad de la actividad neuronal y manipulación cerebral

El desarrollo y uso de neurotecnologías buscará contribuir al derecho de toda persona a gozar de una vida digna, junto a los beneficios del progreso científico y tecnológico, preservando los derechos relativos a la identidad, autonomía, el libre desarrollo de la personalidad y la intimidad.

La actividad neuronal genera la totalidad de las actividades mentales y cognitivas de los seres humanos, y por ello forma parte de la esencia de la persona, su identidad y privacidad, por lo tanto está protegida por las normas de derechos humanos. Cada persona tiene una configuración neuronal única. Es fundamental preservar y garantizar el control de cada persona sobre su propia identidad individual, así como asegurar la autodeterminación y la libertad de pensamiento de las personas.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Las personas tienen derecho a decidir sobre su propia identidad cerebral natural y a que su cerebro no sea manipulado artificialmente para que sus decisiones y su personalidad sean propias y no fruto de la manipulación artificial de su cerebro.

Queda prohibido manipular artificialmente el cerebro o la información neuronal con finalidad diferente a la promoción de la salud, el diagnóstico, tratamiento, rehabilitación y paliación de la enfermedad 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.

Artículo 5. Ética y protección de los Derechos Humanos desde el diseño y por defecto de las neurotecnologías.

El Estado promoverá un enfoque basado en Derechos Humanos en el desarrollo de las neurotecnologías, buscando garantizar la protección integral y el respeto a los derechos humanos a partir del diseño de las neurotecnologías, sus modos de investigación, como en su implementación, comercialización, evaluación y uso.

La protección de los derechos humanos desde el diseño implica, entre otras, lo siguiente:

a) Previo al estudio o investigación neuronal o al diseño y desarrollo de neurotecnologías o productos, se debe efectuar una evaluación de impacto en los derechos humanos , con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar la protección de los derechos humanos
b) Dicha evaluación deberá incluir, como mínimo, lo siguiente: (1) Una descripción detallada de las operaciones de tratamiento de datos neuronales que involucra el estudio o investigación; (2) Una evaluación de los riesgos específicos para los derechos y libertades de las personas; (3) Las medidas preventivas para afrontar/mitigar los riesgos sobre los

Con el apoyo de:
Con el apoyo de:
Cooperación Española

derechos fundamentales, y (4) Los controles que se adoptarán para verificar la pertinencia, oportunidad y efectividad de las medidas a que se refiere el numeral anterior.

Desde antes que se recolecten neurodatos y durante todo el ciclo de vida de los mismos, se deberán adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con el objeto de evitar vulneraciones a los derechos fundamentales y usos indebidos de dicha información o de las neurotecnologías.

La ética desde el diseño y por defecto debe irradiar el esquema, desarrollo y uso de los productos o procesos de investigación sobre el cerebro, las neurotecnologías y los neurodatos.

Todo estudio, ensayo o protocolo de investigación debe tomar en consideración las normas, pautas y guías de ética en investigación.

Artículo 6. Principio de precaución

En caso de existir elementos que permitan considerar la posibilidad de que se genere un daño grave e irreversible para el ser humano o la dignidad humana asociados a la investigación o uso de neurotecnologías o los neurodatos, aun cuando no exista certeza científica de las relaciones causa efecto, se deben tomar medidas precautorias para evitar que se cause dicho daño.

El principio de precaución también aplica cuando el riesgo o la magnitud del daño producido o que puede sobrevenir no son conocidos con anticipación.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 7. Los datos neuronales como datos personales altamente sensibles.

Los neurodatos constituyen datos personales altamente sensibles. Las personas responsables o encargadas del tratamiento y uso de los datos neuronales adoptarán medidas de privacidad y de seguridad reforzadas, asegurando límites en la aplicación de las técnicas de descodificación que permitan identificar a una persona o hacerla identificable, especialmente con bases de datos o conjuntos de información que sean compartidos con terceras partes. El Estado fomentará medidas para garantizar el dominio, la seguridad, confidencialidad e integridad de los neurodatos. El enfoque en el tratamiento de neurodatos deberá estar enmarcado en el derecho a la protección de datos personales.

Artículo 8. Responsabilidad demostrada y seguridad en el tratamiento de neurodatos

Respecto de los neurodatos es fundamental adoptar medidas útiles, oportunas, pertinentes, eficaces y demostrables para el cumplimiento de la presente ley. En especial medidas que eviten: accesos, circulación, suministro y usos indebidos o no autorizados, así como manipulación y destrucción de los neurodatos.

Todas las medidas de seguridad, deben ser objeto de revisión, evaluación y mejoras permanentes.

Artículo 9. Consentimiento expreso e informado para el tratamiento de los neurodatos

El consentimiento previo de la persona titular de los datos neuronales es un requisito imprescindible para la recolección y el tratamiento de esa información. Este debe ser libre, informado, expreso, específico, inequívoco y debe tener por objeto una finalidad lícita y específica. El consentimiento otorgado puede ser revocable en todo momento, con excepción cuando el neurodato se ha disociado irreversiblemente de la identidad. Se requieren medidas de protección específicas cuando

Con el apoyo de:
Con el apoyo de:
Cooperación Española

los titulares de los datos sean sujetos de especial protección como, entre otros, niñas, niños y adolescentes, personas con discapacidad, mayores adultos o privadas de la libertad.

Artículo 10. Igualdad, no Discriminación y acceso equitativo a las neurotecnologías.

Deberá hacerse todo lo posible por garantizar que los neurodatos o las neurotecnologías no se utilicen con fines que discriminen, estigmaticen o violen los derechos y libertades humanas. El diseño de neurotecnologias asociadas a inteligencia artificial deberá proteger a las personas de sesgos discriminatorios.

El Estado promoverá el desarrollo y uso de las neurotecnologías, accesibles a todas las personas, desde un enfoque diferencial, conforme al principio de igualdad, no discriminación y el acceso equitativo. Además, deberá desarrollar políticas públicas de innovación responsable, procurando avanzar hacia el cierre de las brechas de desigualdad y discriminación, particularmente en los grupos de especial protección.

Con el fin de garantizar la participación de las personas en condición de discapacidad en tratamiento de neurodatos y el uso de neurotecnologías se deberán adoptar los ajustes razonables para la toma decisiones y el acceso en condiciones de igualdad y equidad.

Artículo 11. Aplicación terapéutica exclusiva respecto al aumento de las capacidades cognitivas.

El uso de las tecnologías deberá responder a las finalidades de la medicina, es decir la promoción de la salud, la prevención, diagnóstico, tratamiento rehabilitación y cuidados paliativos de la enfermedad.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

El Estado procurará regular con especial cautela el uso de las neurotecnologías para aumentar o mejorar las habilidades cognitivas de las personas o alterar su naturaleza humana. Se deben establecer límites claros y ejercer un control reforzado. Teniendo especial cuidado y precaución respecto de aquellos supuestos que más allá de su aplicación terapéutica o del ámbito de salud pretendan el estudio y uso de neurotecnologías para el aumento o la mejora de las capacidades cognitivas para otros fines.

Artículo 12. Integridad neurocognitiva

Es indispensable garantizar la protección de la integridad neurocognitiva, física y mental, de todas las personas y prevenir su uso para fines ilegítimos o maliciosos que resulten en intervenciones neurotecnológicas destinadas al daño o afectación de la actividad cerebral o que impacten en el ejercicio de los derechos humanos. El acceso a la actividad cerebral nunca podrá alterar la libertad de pensamiento y conciencia, haciendo que el individuo sea dependiente de un tercero, afectando sus ideas, seguridad e independencia, así como su identidad y continuidad psicológica. Toda persona tiene derecho a no sufrir violaciones, alteraciones, manipulaciones y/o modificaciones de su integridad e intimidad neurocognitiva que ponga en riesgo o afecte la integridad personal. Se garantiza la protección a la integridad neurocognitiva en los tratamientos neurotecnológicos, estando prohibidos mecanismos compulsivos o forzosos de aplicación, así como su uso como método de tortura o tratamiento cruel, inhumano o degradante.

Artículo 13. Gobernanza transparente de las neurotecnologías.

El Estado procurará asegurar que todos los actores –tanto estatales como no estatales– que estén vinculados con el desarrollo, uso y/o comercialización de neurotecnologías garanticen la transparencia de los avances neurotecnológicos. Esto comprende tanto la manera en que se estudian, desarrollan, aplican y funcionan las neurotecnologías, como su compatibilidad con los derechos humanos, la protección de los neuroderechos, y la rendición de cuentas sobre el tratamiento de los neurodatos.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 14. Supervisión y fiscalización de las neurotecnologías.

El Estado ejercerá supervisión para garantizar que el uso y la aplicación de las neurotecnologías se desarrolle conforme a los estándares internacionales en materia de derechos humanos a efectos de evitar y prevenir los riesgos e impactos negativos en los derechos de las personas, teniendo especial cuidado en la protección de derechos en niñas, niños y adolescentes y personas con discapacidad y personas privadas de libertad.

Artículo 15. Protección efectiva de los derechos.

El Estado garantizará la existencia de mecanismos de tutela efectiva de los derechos asociados al desarrollo y uso de las neurotecnologías. También garantizará el acceso a acciones judiciales y reparaciones integrales en el caso de vulneraciones a los derechos humanos, a efectos de promover una efectiva protección de estas garantías, de conformidad con los presentes Principios.

Artículo 16. Solidaridad , cooperación y beneficios compartidos.

Los beneficios resultantes de toda investigación científica en el área de las neurociencias y las neurotecnologías así como sus aplicaciones deben compartirse con la sociedad en su conjunto.

Artículo 17. Protección de las generaciones futuras.

Las generaciones actuales tienen la responsabilidad de garantizar la protección de las generaciones futuras. En la investigación y aplicación de las neurotecnologías se debe asegurar la preservación de la especie humana, la dignidad y derechos humanos así como la diversidad biológica y cultural. Los neurodatos hacen parte del patrimonio común de la humanidad.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Es necesario considerar una adecuada gestión de riesgo y la aplicación del principio de precaución en la toma de decisiones.

Artículo 18. Gratuidad y no comercialización.

Los neurodatos no pueden ser objeto de lucro, comercio o enriquecimiento de terceros. Estos pueden ser cedidos con fines de investigación, lo que implica que el titular de los datos renuncia a compensaciones de naturaleza económica.

Se prohíbe que las personas renuncien a sus neurodatos o que la actividad neuronal se escriba directamente en sus cerebros para obtener una recompensa financiera.

Artículo 19. Transferencia de tecnología y conocimientos.

En la medida de lo posible, se deberá buscar que se generen estrategias encaminadas a fortalecer la capacidad científica y tecnológica del país mediante la transferencia de tecnología y conocimiento desde los creadores y desarrolladores de este tipo de neurotecnologías

Anexo 2 : Propuesta de Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales

CONVENCIÓN INTERAMERICANA SOBRE AUTODETERMINACIÓN INFORMATIVA, TRATAMIENTO Y CIRCULACIÓN DE DATOS PERSONALES

Con el apoyo de:
Con el apoyo de:
Cooperación Española

LOS ESTADOS PARTE DE LA PRESENTE CONVENCIÓN,

RECONOCIENDO que el respeto irrestricto a los derechos humanos y a la privacidad ha sido consagrado en la Declaración Americana de los Derechos y Deberes del Hombre y en la Declaración Universal de los Derechos Humanos y reafirmado en otros instrumentos internacionales y regionales;

RECORDANDO los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales redactados por el Comité Jurídico de la OEA en 2021 y afirmando que la protección de los datos personales trasciende a todos los sectores de la sociedad independientemente de su nacionalidad, residencia, clase, raza o etnia, nivel de ingresos, cultura, educación, edad o religión;

RECORDANDO que la Corte interamericana de Derechos Humanos ha reconocido el derecho a la autodeterminación informativa como un derecho autónomo en la sentencia Serie C No. 506 de 18 de octubre de 2023;

AFIRMANDO que la vulneración de los derechos a la privacidad y a la protección de los datos personales es una violación de los derechos humanos y las libertades fundamentales y limita total o parcialmente a los titulares de datos el reconocimiento, goce y ejercicio de tales derechos y libertades y de otros derechos humanos;

PREOCUPADOS porque la tecnología de la información esté al servicio de cada ciudadano, el desarrollo de la sociedad de la información se dé en el marco de la cooperación internacional y que ninguna tecnología atente contra los derechos humanos, ni la tutela de los datos personales, ni constituya una ofensa a la dignidad humana;

PREOCUPADOS porque cada vez son más frecuentes los incidentes de seguridad en los sectores público y privado, amenazan en la región la seguridad de los ciudadanos y les impiden disfrutar adecuadamente los beneficios del gobierno electrónico, de los servicios digitales y del desarrollo sostenible por medio de la tecnología de la información;

Con el apoyo de:
Con el apoyo de:
Cooperación Española

CONVENCIDOS de que elevar el nivel de protección de los datos personales es una prioridad para la región y una condición indispensable para el desarrollo individual y social y su plena e igualitaria participación en todas las esferas de la sociedad de la información,

HAN CONVENIDO en lo siguiente:

CAPÍTULO I - ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1. Objetivos

1.1. La presente Convención tiene por objeto:

a) Fijar las reglas para garantizar el debido tratamiento de los datos personales y proteger los derechos de las personas titulares de esa información.

b) Facilitar el flujo de los datos personales entre los Estados miembros con la finalidad de coadyuvar al crecimiento social y económico y el desarrollo sostenible de la región.

c) Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados miembros, las autoridades de control no pertenecientes al Convenio y autoridades y entidades internacionales en la materia.

1.2. La protección de datos personales se basa en:

a. el respeto a la privacidad reconocido en el art. 11 de la Convención Americana de Derechos Humanos;

b. el derecho a la autodeterminación informativa;

c. la libertad de expresión, información, comunicación y opinión;

Con el apoyo de:
Con el apoyo de:
Cooperación Española

d. la inviolabilidad de la intimidad, del honor y de la imagen;

e. el desarrollo e innovación económica y tecnológica;

f. la libre empresa, libre competencia y protección del consumidor;

g. los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas naturales.

Artículo 2. Definiciones

2.1. Para los efectos de esta Convención debe entenderse por:

a. Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

b. Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

c. Datos personales: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

d. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan, entre otros, revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

e. Encargado: prestador de servicios que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de este.

f. Exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

g. Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

h. Titular del dato personal: persona física a quien le conciernen los datos personales.

i. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Artículo 3. Ámbito de aplicación subjetivo

3.1. Las obligaciones y derechos establecidos en esta Convención serán aplicables a las personas físicas, autoridades y organismos públicos que traten datos personales en el ejercicio de sus actividades y funciones.

3.2. Las obligaciones y derechos establecidos en esta Convención serán aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos

soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

3.3. Las obligaciones y derechos establecidos en esta Convención serán aplicables a los datos personales de personas físicas, lo cual no impide que los Estados miembros en su legislación nacional dispongan que la información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales, en cumplimiento a lo establecido en su derecho interno.

3.4. Las obligaciones y derechos establecidos en esta Convención no son aplicables en los siguientes supuestos:

a. Cuando los datos personales estén destinados a actividades exclusivamente internas en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como finalidad una divulgación o utilización comercial de dichos datos.

b. La información anónima en su origen, es decir, aquella que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado.

Artículo 4. Ámbito de aplicación territorial

4.1. Los derechos reconocidos en esta Convención serán aplicables al tratamiento de datos personales efectuado:

a. Por un responsable o encargado establecido en territorio de los Estados miembros.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

b. Por un responsable o encargado no establecido en territorio de los Estados miembros, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados miembros, o bien, estén relacionadas con el control de su comportamiento, en la medida en que este tenga lugar en los Estados miembros.

c. Por un responsable o encargado que no esté establecido en un Estado miembro pero que le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud de los principios del derecho internacional público.

d. Por un responsable o encargado no establecido en territorio de alguno de los Estados miembros y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

4.2. Para los efectos de esta Convención, se entenderá por establecimiento el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, con naturaleza estable y permanente.

4.3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del responsable o encargado.

CAPÍTULO II - PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

Artículo 5. Principio de dignidad humana

Los Estados adoptarán medidas necesarias y eficaces, incluso de orden legislativo, para garantizar que todo los desarrollos científicos o tecnológicos sean en beneficio de la dignidad humana, los derechos humanos, las libertades fundamentales, la sociedad y la humanidad.

Artículo 6. Principio de legitimación

6.1. Por regla general, el responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos:

a. El titular otorgue su consentimiento expreso para una o varias finalidades específicas.

b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.

d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.

f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.

h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.

i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los

derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones legales.

Artículo 7. Principio del consentimiento

7.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

7.2. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.

Artículo 8. Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes

8.1. En la obtención del consentimiento de niñas, niños y adolescentes, el responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de los Estados miembros, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno de cada Estado miembro ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela.

8.2. El responsable realizará esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad o tutela, o bien, por el menor directamente atendiendo a su edad de acuerdo con el derecho interno de cada Estado-miembro, teniendo en cuenta la tecnología disponible.

8.3. El tratamiento de datos personales de niños, niñas y adolescentes debe realizarse en su interés superior, de conformidad con el artículo 21 de esta Convención.

Artículo 9. Principio de licitud

9.1. El responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado-miembro que resulte aplicable, el derecho internacional y los derechos y libertades de las personas.

9.2. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado-miembro de que se trate les confiera expresamente, además de lo previsto en el artículo anterior de esta Convención.

Artículo 10. Principio de lealtad y buena fe

10.1. El responsable o encargado del tratamiento deberá actuar en pleno respeto del principio de buena fe. En este sentido, el responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar estos a través de medios engañosos o fraudulentos.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

10.2. Para los efectos de la presente Convención, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

Artículo 11. Principio de transparencia

11.1. El responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

11.2. El responsable proporcionará al titular, al menos, la información siguiente:

a. Su identidad y datos de contacto.

b. Las finalidades del tratamiento a que serán sometidos sus datos personales.

c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.

d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos definidos por el Artículo 20 de esta Convención.

e. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

11.3. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

11.4. Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

Artículo 12. Principio de finalidad

12.1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

12.2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquellas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

12.3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos en favor del interés público, no se considerará incompatible con las finalidades iniciales.

Artículo 13. Principio de minimización

13.1. El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

Artículo 14. Principio de calidad

14.1. El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de estos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento. La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada y comprobable. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

14.2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

14.3. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de estos.

14.4. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquellas relacionadas con exigencias legales aplicables al responsable. No obstante, la legislación nacional de los Estados miembros aplicable en la materia podrá establecer excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular.

Artículo 15. Principio de responsabilidad demostrada

Con el apoyo de:
Con el apoyo de:
Cooperación Española

15.1. El responsable implementará los mecanismos útiles, pertinentes, eficaces y oportunos que sean necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente Convención, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

15.2. Lo anterior aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

15.3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

15.4. El responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

Artículo 16. Principio de seguridad

16.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, humano, contractual, físico, técnico y de cualquier otra naturaleza que sean suficientes para, de una parte, garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos personales y, de otra parte, evitar la pérdida, manipulación, consulta, uso o acceso no autorizado o fraudulento de dicha información.

En el caso de datos personales sensibles y de niñas, niños o adolescentes, implementará medidas más estrictas para garantizar la seguridad y confidencialidad de la información (seguridad reforzada).

16.2. Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:

a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

b. El estado de la técnica.

c. Los costos de aplicación.

d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

e. El alcance, contexto y las finalidades del tratamiento.

f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.

g. El número de titulares involucrados.

h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.

i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.

16.3. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

Artículo 17. Notificación de vulneraciones a la seguridad de los datos personales

17.1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.

17.2 Adicionalmente, deberá adoptar las medidas necesarias para evitar que cualquier incidente de seguridad cause daño a los titulares de los datos, o que, según el caso, el mismo sea el mínimo posible.

17.3. Lo anterior no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o

bien, que esta no represente un riesgo para los derechos y las libertades de los titulares involucrados.

17.4. La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo.

17.5. La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.

b. Los datos personales comprometidos.

c. Las acciones correctivas realizadas de forma inmediata.

d. Las recomendaciones al titular sobre las medidas que este pueda adoptar para proteger sus intereses.

e. Los medios disponibles al titular para obtener mayor información al respecto.

17.5. El responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad de control.

17.6. La legislación nacional de los Estados miembro aplicable en la materia establecerá los efectos de las notificaciones de vulneraciones de seguridad que realice el responsable a la autoridad de

control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con la finalidad de salvaguardar los intereses, derechos y libertades de los titulares afectados.

Artículo 18. Principio de confidencialidad

18.1. El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.

Artículo 19. Principio de prevención y precaución

19.1. Los responsables y encargados del tratamiento de datos personales deberán implementar medidas preventivas para evitar daños o perjuicios a los titulares de los datos, o vulnerar sus derechos. Cuando el tratamiento de datos personales sea susceptible de causar un daño grave e irreversible, el responsable o encargado del tratamiento deberá abstenerse de realizar dicho tratamiento o adoptar medidas precautorias o preventivas para proteger los derechos del titular del dato, su dignidad humana y otros derechos humanos.

19.2. Asimismo, el responsable o encargado del tratamiento deberá abstenerse de realizar dicho tratamiento o adoptar las medidas adecuadas para proteger los derechos del titular o titulares de los datos, su dignidad humana y otros derechos humanos con base en el principio de precaución. Este principio se aplica cuando el riesgo o la magnitud del daño producido o que puede sobrevenir no son conocidos con anticipación, porque no hay manera de establecer, a mediano o largo plazo, los efectos de un tratamiento de datos.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

19.3. Para identificar riesgos, el responsable y el encargado deben realizar una evaluación de impacto preliminar e, idealmente, probar las actividades de tratamiento propuestas en entornos controlados para la experimentación y la innovación, como sandboxes.

CAPÍTULO III - DERECHOS PROTEGIDOS

Artículo 20. Derecho a la autodeterminación informativa y protección de los datos personales

20.1. Toda persona tiene derecho a la autodeterminación informativa y la protección de sus datos personales de conformidad con las normas de esta Convención. Dichos derechos se concretan en la facultad de toda persona para ejercer control sobre sus datos personales, que se tratarán de modo legítimo, licito, leal, transparente, seguro, responsable, confidencial, para fines explícitamente definidos sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.

20.2. A toda persona cuyos datos sean tratados son garantizados los derechos definidos por el Artículo 21 de esta Convención. Las autoridades reguladoras independientes designadas por cada Estado miembro son responsables para garantizar el pleno respeto de estos derechos.

Artículo 21. Derechos

21.1. Toda persona tendrá derecho a:

a. No estar sujeta a una decisión que la afecte significativamente, basándose únicamente en un tratamiento automatizado de datos sin considerar sus opiniones. Esta norma no será aplicable si la decisión ha sido autorizada por una ley a la cual el responsable del tratamiento está sujeto siempre y cuando esta ley establezca medidas apropiadas para garantizar los derechos, las libertades e intereses legítimos del titular de datos;

b. Obtener, cuando así lo solicitare, en intervalos razonables y sin demora o gastos excesivos, confirmación del tratamiento de los datos personales relacionados con su persona, la comunicación en forma inteligible de los datos tratados, toda la información disponible sobre su origen, el período de conservación así como cualquier otra información que el responsable del tratamiento deba proporcionar con el fin de asegurar la transparencia del tratamiento incluyendo las medidas de seguridad adoptadas sobre sus datos personales;

c. Obtener, cuando así lo solicitare, conocimiento del razonamiento subyacente al tratamiento de datos cuando los resultados de dicho tratamiento se le aplicaren;

d. Oponerse en cualquier momento, por fundamentos relacionados con su situación, al tratamiento de datos personales que la involucren, salvo si el responsable del tratamiento demostrara fundamentos legítimos para el tratamiento superiores a sus intereses o derechos o libertades fundamentales;

e. Obtener, cuando así lo solicitare, exenta de costos y sin demoras excesivas, la rectificación o eliminación, según sea el caso, de dichos datos si estos estuvieron siendo o hubieren sido tratados en forma contraria a las disposiciones de la presente Convención;

f. Obtener una solución jurídica según lo previsto en el Artículo 26 de esta Convención cuando sus derechos de conformidad con la presente Convención hubieren sido violados;

g. Beneficiarse, cualquiera sea su nacionalidad o residencia, de la asistencia de una autoridad de control según lo dispuesto en el Artículo 27 de esta Convención, para ejercer sus derechos de conformidad con la presente Convención.

h. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura

mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

i. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tiene derecho a solicitar la revisión de decisiones adoptadas únicamente sobre la base del tratamiento automatizado de datos personales que afecten a sus intereses, incluidas las decisiones destinadas a definir su perfil personal, profesional, de consumo y crediticio o aspectos de su personalidad. Consiguientemente, el responsable del tratamiento deberá brindar, cuando se le solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, observando secretos comerciales e industriales

j. Los Estados miembros deben adoptar, en la medida de lo posible, el derecho a la revisión humana de la toma de decisiones automatizadas.

21.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

21.3. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

21.4. Los Estados miembros deberán otorgar a toda persona recursos judiciales efectivos para la tutela de los derechos reconocidos en esta Convención, incluida la indemnización por el tratamiento no autorizado de sus datos personales o en infracción a los derechos reconocidos.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

21.5. La legislación nacional de los Estados miembros aplicable en la materia reconocerá el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de su derecho a la protección de datos personales.

21.6. El derecho interno de los Estados miembros señalará la autoridad competente para conocer de este tipo de acciones interpuestas por el titular afectado, así como los plazos, requerimientos y términos a través de los cuales será indemnizado este, en caso de resultar procedente.

Artículo 22. Tratamiento de datos personales de niñas, niños y adolescentes

22.1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes, los Estados miembros de esta Convención deberán privilegiar 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.

22.2. Los Estados miembros promoverán en la formación académica de las niñas, niños y adolescentes el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

Artículo 23. Tratamiento de datos personales de carácter sensible

Con el apoyo de:
Con el apoyo de:
Cooperación Española

23.1. Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:

a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.

b. Se dé cumplimiento a un mandato legal.

c. Se cuente con el consentimiento expreso y por escrito del titular.

d. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

23.2. La legislación nacional de los Estados miembros aplicable en la materia podrá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno.

Artículo 24. Excepciones y restricciones

24.1. No se permitirá excepción alguna a las disposiciones establecidas en este Capítulo, salvo que dicha excepción se encuentre prevista por la ley, respete la esencia de los derechos consagrados en esta Convención y las libertades fundamentales y constituya una medida necesaria y proporcionada en una sociedad democrática para:

a. Proteger la seguridad nacional, la defensa, la seguridad pública, los intereses económicos y financieros importantes del Estado, la imparcialidad e independencia del poder judicial o la prevención, investigación y procesamiento de delitos, así como la aplicación de sanciones penales, y otros objetivos esenciales de interés público general;

b. Proteger al titular de datos o los derechos y las libertades fundamentales de otros, en particular, la libertad de expresión.

24.2. Las restricciones para ejercer las disposiciones especificadas en los Artículos 18 y 19 deben ser previstas por la ley, con respecto al tratamiento de datos con la finalidad de archivo en interés público, investigaciones científicas o históricas o finalidades estadísticas cuando no exista riesgo identificable de violación de los derechos y las libertades fundamentales de los titulares de datos.

24.3. Las actividades de tratamiento con finalidades de seguridad nacional y defensa están sujetas a revisión y supervisión independiente y efectiva, según las leyes locales de la Parte pertinente.

CAPÍTULO IV - OBLIGACIONES

Artículo 25. Obligaciones

25.1. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento tomen todas las medidas necesarias para cumplir con las obligaciones de la presente Convención y sean capaces de demostrar, sujetos a las leyes locales, que el tratamiento de datos bajo su control cumple con las disposiciones de la presente Convención.

25.2. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento examinen el probable impacto del tratamiento de datos sobre los derechos y las libertades fundamentales de los titulares de datos, previo al comienzo de dicho tratamiento, y deberán diseñar el tratamiento de datos de manera tal que se prevenga o minimice el riesgo de interferencia con dichos derechos o libertades fundamentales.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

25.3. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento implementen medidas técnicas y organizacionales que tomen en cuenta las implicancias del derecho a la protección de datos personales en todas las etapas del tratamiento de datos.

25.4. Cada Parte podrá, teniendo en consideración los riesgos con relación a los intereses, derechos y libertades fundamentales de los titulares de datos, adaptar la aplicación de las disposiciones de los párrafos 1, 2 y 3 en la ley que dote de eficacia a las disposiciones de la presente Convención, según la naturaleza y el volumen de los datos, la naturaleza, el alcance y la finalidad del tratamiento y, si correspondiere, el tamaño del responsable del tratamiento o encargado del tratamiento.

CAPÍTULO V – TRANSFERENCIA Y RECOLECCIÓN INTERNACIONAL DE DATOS PERSONALES

Artículo 26. Reglas generales para las transferencias de datos personales

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

a. El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de este que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado, siendo el respeto de las disposiciones de esta Convención considerado como garantía de tales condiciones mínimas y suficientes.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

b. El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y este, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado miembro aplicable en la materia.

c. El exportador y el 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. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados aplicable en la materia.

d. El exportador y el destinatario adopten un esquema de códigos corporativos vinculantes o un mecanismo de certificación aprobado, siempre y cuando este sea acorde con las disposiciones previstas en la legislación nacional del Estado miembro aplicable en la materia, que está obligado a observar el exportador.

e. La autoridad de control del Estado miembro del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

26.2. La legislación nacional de los Estados miembros aplicable en la materia podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

27. Recolección internacional de datos personales

27.1. 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 es recolectada desde terceros países por parte de responsables o encargados ubicados en países diferentes al del domicilio o residencia del titular del dato personal y que no tienen sede física o establecimiento en el mismo (recolector internacional de datos).

Con el apoyo de:
Con el apoyo de:
Cooperación Española

27.2. 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.

27.3. La no presencia, residencia física o establecimiento del recolector internacional de datos en el país del titular del dato no podrá ser una excusa para el incumplimiento de las obligaciones o la falta de protección de los derechos definidos en esta Convención.

CAPÍTULO VI - AUTORIDADES DE CONTROL

Artículo 28. Naturaleza de las autoridades de control y supervisión

28.1. En cada Estado miembro deberán existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia.

28.2. Las autoridades de control podrán ser órganos unipersonales o pluripersonales; actuarán con carácter imparcial e independiente en sus potestades, así como serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna.

28.3. El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos

personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Sus funcionarios se nombrarán mediante un procedimiento transparente en virtud de la legislación nacional aplicable y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado miembro, conforme a las reglas del debido proceso.

28.4. La legislación nacional de los Estados miembros que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, auditoría, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de esta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

28.5. Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados miembros que resulte aplicable en la materia y su derecho interno.

28.6. Las autoridades de control deberán contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

Artículo 29.- Régimen de reclamaciones y de imposición de sanciones

29.1. Todo titular tendrá derecho a presentar su reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación nacional del Estado miembro que resulte aplicable en la materia, incluyendo la solicitud de cese de la conducta violatoria de esta Convención, medidas cautelares para detener el daño y la indemnización de los perjuicios de cualquier índole ocasionados por el tratamiento ilegal de datos personales.

29.2. La legislación nacional de los Estados miembros aplicable en la materia establecerá un régimen que permita al titular presentar una reclamación ante la autoridad de control cuando considere que el tratamiento de sus datos personales infringe la normativa nacional en la materia, así como a solicitar la tutela judicial.

29.3. La legislación nacional de los Estados miembros aplicable en la materia establecerá un régimen que permita la adopción de medidas correctivas y sancionar las conductas que contravengan lo dispuesto en las legislaciones nacionales correspondientes, indicando, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones, a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia.

CAPÍTULO VII - MECANISMOS INTERAMERICANOS DE PROTECCIÓN

Artículo 30.- Comisión Interamericana de Protección de Datos Personales

30.1. La Comisión Interamericana de Protección de Datos Personales funcionará como un órgano autónomo y estará encargada de la promoción y protección de los derechos reconocidos en esta Convención en los países miembros. Estará integrada por las autoridades de protección de datos de los países miembros de la Convención, las que actuarán ad honorem.

30.2. La Comisión Interamericana de Protección de Datos Personales adoptará su propio reglamento interno.

30.3. La Comisión Interamericana de Protección de Datos Personales tendrá una Secretaría General que tendrá carácter administrativo del Convenio y será ejercida en forma rotativa y por el plazo de

dos años por alguna de las autoridades de protección de datos de los países miembros de la Convención. Inicialmente la Secretaría General estará a cargo de la autoridad de protección de datos del primer Estado miembro que ratifique el Convenio y lo notifique a los otros Estados firmantes.

30.4. La función de Secretario General de la Comisión Interamericana de Protección de Datos Personales es ejercida, de manera rotativa y por el plazo de dos años, por el presidente de la misma autoridad que ejerce la Secretaria General rotativa.

30.5. Sus funciones son:

a. Facilitar la comunicación, cooperación y coordinación entre las autoridades nacionales de protección de datos de los países miembros.

b. Elaborar un informe anual del estado de la protección de datos en la región;

c. Preparar documentos, opiniones y guías sobre la aplicación e interpretación de la convención;

d. Colaborar con los Estados miembros en la implementación del tratado en sus leyes locales, sin perjuicio de las normas que resulten directamente aplicables.

e. Recibir los instrumentos de ratificación del Convenio y las propuestas de modificación del mismo.

Artículo 31.- Informes

31.1. Con la finalidad de proteger el derecho de las personas a la tutela de sus datos personales, en los informes nacionales a la Comisión Interamericana de Protección de Datos Personales, los Estados parte deberán incluir información sobre las medidas adoptadas para prevenir y hacer respetar los derechos reconocidos en este Convenio, así como sobre las dificultades que observen en la

aplicación de las mismas y los factores que contribuyan a la adecuada tutela de los datos personales.

Artículo 32 - Opiniones consultivas

32.1. Los Estados parte en esta Convención y las respectivas agencias de protección de datos personales podrán requerir a la Comisión Interamericana de Protección de Datos Personales opinión consultiva sobre la interpretación de esta Convención.

Artículo 33 - Recursos

33.1. Cualquier persona o grupo de personas, o entidad no gubernamental legalmente reconocida en uno o más Estados miembros de la Organización, puede presentar a la Comisión Interamericana de Protección de Datos Personales peticiones que contengan denuncias o quejas de violación de los derechos previstos en la presente Convención por un Estado parte, y la Comisión las considerará de acuerdo con las normas y los requisitos de procedimiento para la presentación y consideración de peticiones estipulados en su propio reglamento interno.

CAPÍTULO VIII - DISPOSICIONES GENERALES DEL CONVENIO

Artículo 34

34.1. Nada de lo dispuesto en la presente Convención podrá ser interpretado como restricción o limitación a la legislación interna de los Estados parte que prevea iguales o mayores protecciones y garantías de los derechos del titular de los datos personales.

Artículo 35

35.1. Nada de lo dispuesto en la presente Convención podrá ser interpretado como restricción o limitación a la Convención Americana sobre Derechos Humanos o a otras convenciones internacionales sobre la materia que prevean iguales o mayores protecciones relacionadas con este tema.

Artículo 36

36.1. La presente Convención está abierta a la firma de todos los Estados del continente americano.

Artículo 37

37.1. La presente Convención está sujeta a ratificación.

Artículo 38

38.1. La presente Convención queda abierta a la adhesión de cualquier otro Estado.

Artículo 39

39.1. Los Estados no podrán formular reservas a la presente Convención al momento de aprobarla, firmarla, ratificarla o adherirse a ella.

Artículo 40

40.1. Cualquier Estado parte puede someter a los otros Estados miembros de la Convención una propuesta de enmienda a esta Convención. Las enmiendas entrarán en vigor para los Estados ratificantes de las mismas en la fecha en que dos tercios de los Estados parte hayan depositado el respectivo instrumento de ratificación. En cuanto al resto de los Estados parte, entrarán en vigor en la fecha en que depositen sus respectivos instrumentos de ratificación.

Artículo 41

41.1. Los Estados parte que tengan dos o más unidades territoriales en las que rijan distintos sistemas jurídicos relacionados con cuestiones tratadas en la presente Convención podrán declarar, en el momento de la firma, ratificación o adhesión, que la Convención se aplicará a todas sus unidades territoriales o solamente a una o más de ellas. Tales declaraciones podrán ser modificadas en cualquier momento mediante declaraciones ulteriores, que especificarán expresamente la o las unidades territoriales a las que se aplicará la presente Convención.

Artículo 42

42.1. La presente Convención entrará en vigor el trigésimo día a partir de la fecha en que se haya depositado el primer instrumento de ratificación. Para cada Estado que ratifique o adhiera a la Convención después de haber sido depositado el segundo instrumento de ratificación, entrará en vigor el trigésimo día a partir de la fecha en que tal Estado haya depositado su instrumento de ratificación o adhesión.

Artículo 43

43.1. El Secretario General de la Comisión Interamericana de Protección de Datos Personales informará a todos los Estados miembros de la Organización de los Estados Americanos de la entrada en vigor de la Convención.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Artículo 44

44.1. La Comisión Interamericana de Protección de Datos Personales presentará un informe anual a los Estados miembros de la Comisión Interamericana de Protección de Datos Personales sobre el estado de esta Convención, inclusive sobre las firmas, depósitos de instrumentos de ratificación, adhesión o declaraciones, así como las reservas que hubieren presentado los Estados parte y, en su caso, el informe sobre las mismas.

Artículo 45

45.1. La presente Convención regirá indefinidamente, pero cualquiera de los Estados parte podrá denunciar esta Convención mediante el depósito de un instrumento con ese fin en la Secretaría General de la Comisión Interamericana de Protección de Datos Personales. Un año después a partir de la fecha del depósito del instrumento de denuncia, la Convención cesará en sus efectos para el Estado denunciante, quedando subsistente para los demás Estados parte.

Artículo 46

46.1. El instrumento original de la presente Convención, cuyos textos en español y portugués son igualmente auténticos, será depositado en la Secretaría General de la Comisión Interamericana de Protección de Datos Personales, la que enviará copia certificada de su texto para su registro y publicación a la Secretaría de las Naciones Unidas, de conformidad con el artículo 102 de la Carta de las Naciones Unidas.

EN FE DE LO CUAL, los plenipotenciarios infrascritos, debidamente autorizados por sus respectivos gobiernos, firman el presente Convenio, que se llamará “Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales”.

Anexo 3 : Listado de documentos sobre protección de datos, neurotecnologías e inteligencia artificial y derechos digitales emitidos por organizaciones internacionales y autoridades de protección de datos

Agencia Española de Protección de Datos (AEPD)

- AEPD (2020). Qué es Iot y cuáles son sus riesgos. En: https://www.aepd.es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos

Asia-Pacific Economic Cooperation (APEC)

- Asia-Pacific Economic Cooperation (2004) Marco de Privacidad APEC (APEC Privacy Framework)

Organización de las Naciones Unidas (ONU)

- ONU (2024). Informe A/79/173 del 17 de julio de 2024: ONU (2024). 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 computarizados de datos personales”.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- ONU. AI Advisory Body (2024).Gobernanza de la IA en beneficio de la humanidad. Informe final (septiembre de 2024).

- ONU (2024). Informe A/HRC/55/46 del 18 de enero de 2024: 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.
- ONU (2023) Informe A/78/310 del 30 de agosto de 2023: 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, Ana Brian Nougrères
- ONU (2022). Informe A/HRC/52/37 del 27 de diciembre de 2022: 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, Ana Brian Nougrères.
- ONU (2022) Informe A/77/196 del 20 de julio de 2022: Principios que informan la privacidad y la protección de datos personales - Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères.
- ONU (2021). Informe A/HRC/46/37 del 25 de enero de 2021: La inteligencia artificial y la privacidad, así como la privacidad de los niños - Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci.
- ONU (1990) Resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de las Naciones Unidas “principios rectores para la reglamentación de los ficheros computadorizados de datos personales”
- ONU (1975) Resolución 3384 de 1975 sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad

Comisión Europea (CE)

- CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52024DC0357 o https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2024%3A357%3AFIN&qid=1721897017650

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- CE, 2024. Joint statement on competition in generative AI foundation models and AI productos (23 July 2024). En:https://competition-policy.ec.europa.eu/document/download/79948846-4605-4c3a-94a6-044e344acc33_en?filename=20240723_competition_in_generative_AI_joint_statement_COMP-CMA-DOJ-FTC.pdf
- CE, 2019. Directrices para una IA fiable. Emitido por el grupo de expertos de alto nivel sobre inteligencia artificial creado por la Comisión Europea

Consejo de Europa (CdE)

- Consejo de Europa (2024). Framework convention on artificial intelligence and human rights, democracy and the rule of law.
- Consejo de Europa (2023). El Consejo de Europa y la inteligencia artificial. Visión global de las actividades del Consejo de Europa en el ámbito de la inteligencia artificial.
- Consejo de Europa (2021). Possible elements of a legal framework on artificial intelligence, based on the Council of Europe´s standards on human rights, democracy and the rule of law (Comité sobre inteligencia artificial -CAI-)
- Council of Europe (2021) Report 'Common Human Rights challenges raised by different applications of neurotechnologies in the biomedical field', October.
- Consejo de Europa (2021). Declaración sobre la necesidad de proteger a los niños en el entorno digital. (Comité consultivo para la protección de las personas en relación con el convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal -T-PD-)
- Consejo de Europa (2021). Recomendación sobre la protección de las personas con respecto al tratamiento automático de datos de carácter personal en el contexto de la elaboración de perfiles. (Comité consultivo para la protección de las personas en relación con el convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal -T-PD-)
- Consejo de Europa (2018). Convenio 108+ para la protección de las personas con respecto al tratamiento de datos de carácter personal.
- Consejo de Europa (2020). Towards regulation of AI systems. (Comité sobre inteligencia artificial -CAI-)
- Consejo de Europa (2020). Handbook for policy makers on the rights of the child in the digital environment. (Comité Directivo de los Derechos del Niño -CDENF-)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Consejo de Europa (2020). Feasibility study on a legal framework on AI design, development and application based on Council of Europe standards. (Comité sobre inteligencia artificial -CAI-)
- Consejo de Europa (2019). Guidelines on artificial intelligence and data protection. (Comité consultivo para la protección de las personas en relación con el convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal -T-PD-)
- Consejo de Europa (2019). Conclusions of AI and its impact on young people seminar (Consejo conjunto sobre la juventud -CMJ-)
- Consejo de Europa (2018). Recommendation on guidelines to respect, protect and fulfil the rights of the child in the digital environment. (Comité Directivo de los Derechos del Niño -CDENF-)
- Consejo de Europa (2017). Guidelines on the protection of individuals with regard to the processing of data in a world of big data. (Comité consultivo para la protección de las personas en relación con el convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal -T-PD-)
- Consejo de Europa (1981). convenio No 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos
- Consejo de Europa (2001). Protocolo adicional del convenio No 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos

Global Privacy Assembly (GPA)

- Global Privacy Assembly (2023) Resolución “Alcanzando estándares globales de protección de datos: principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo”
- Resolución adoptada sobre la rendición de cuentas responsables [y demostrables] en el desarrollo y la utilización de la inteligencia artificial" de la 42ª Sesión Cerrada de la Asamblea Global de Privacidad 2020, celebrada en octubre de 2020.
- Autoridades de Protección de Datos y Privacidad (2009). Estándares internacionales sobre protección de datos personales y privacidad (Resolución de Madrid) -Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad en relación con el Tratamiento de Datos de carácter personal- Madrid, España.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Grupo de trabajo sobre protección de datos del artículo 29

- GTPD 29. Dictamen 8/2014 sobre la evolución reciente de la Internet de los Objetos, adoptados el 16 de septiembre de 2014.
- GTPD 29. Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes

Comité Europeo de Protección de Datos (CEPD)[159]

- CEPD. Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework.
- CEPD. Guideline 01/2023 on article 37 law enforcement directive
- CEPD. Statement 1/2024 on legislative developments regarding the proposal for a regulation laying down rules to prevent and combat child sexual abuse
- CEPD. Guidelines 2/2023 on technical scope of art 5(3) of eprivacy directive
- CEPD. Guidelines 07/2022 on certitication as a tool for transfers
- CEPD. Guidelines 3/2022 on dark patterns in social media platform interfaces: how to recognize and avoid them.
- CEPD. Letter to the European Commission on adapting liability rules to the digital age and artificial intelligence (AI)

[159] https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_es

- CEPD. Guidelines 02/2021 on virtual voice assistans (Directrices 2/2021 sobre los asistentes de voz virtuales)
- CEPD. Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial)
- CEPD. Guiledelines 8/2020 on the targeting of social media users (Directrices 8/2020 sobre la focalización de los usuarios de medio sociales)
- CEPD. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications (Directirces 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad)
- CEPD. Guidelines 4/2019 on article 25 data protection by design and by default (directrices 4/2019 relativas al artículos 25 protección de datos desde el diseño y por defecto)

Organización de Estados Americanos (OEA)

- OEA, 2023. Declaración de principios interamericanos en materia de neurociencias, neurotecnologías y derechos humanos. Aprobada en marzo de 2023 por el Comité Jurídico Interamericano de la Organización de Estados Americanos
- OEA, 2021. Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones expedidos el 9 de abril de 2021 por el Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA). Estos principios fueron aprobados por la Asamblea General de la OEA en noviembre de 2021.
- OEA, 2021. Declaración sobre neurociencia, neurotecnologías y derechos humanos: nuevos desafíos jurídicos para las américas. Aprobada en agosto de 2021 por el Comité Jurídico Interamericano de la Organización de Estados Americanos-

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)

- UNESCO, 2023. Unveiling the neurotechnology landscape. Scientific advancements, innovations and major trends. En: https://unesdoc.unesco.org/ark:/48223/pf0000386137
- UNESCO, 2021. Recomendación sobre la ética de la inteligencia artificial.
- UNESCO, 2021. Ethical issues of neurotechnology: report, adopted in December 2021. En: https://unesdoc.unesco.org/ark:/48223/pf0000383559 v
- UNESCO, 2005. Declaración universal sobre bioética y derechos humanos. Aprobada por aclamación por la 33a sesión de la Conferencia General de la UNESCO, el 19 de octubre de 2005. En: https://unesdoc.unesco.org/ark:/48223/pf0000146180_spa
- UNESCO, 2003. Declaración internacional sobre los datos genéticos humanos. Aprobada por aclamación por la 29 sesión de la Conferencia General de la UNESCO, el 16 de octubre de 2003. En: https://unesdoc.unesco.org/ark:/48223/pf0000253908_spa
- UNESCO, 1997. Declaración universal sobre el genoma humano y los derechos humanos. Aprobada por aclamación por la 29 sesión de la Conferencia General de la UNESCO, el 11 de noviembre de 1997. En: https://unesdoc.unesco.org/ark:/48223/pf0000253908_spa

Organización para la Cooperación y el Desarrollo Económico (OCDE).

- OCDE, 2024. AI, data governance and privacy synergies and areas of international cooperation. OCDE Artificial Intelligence papers. June 2024 no. 22
- OCDE, 2022. Declaration on a Trusted, Sustainable and Inclusive Digital Future.
- OCDE, 2022. Companion Document to the OECD Recommendation on Children in the Digital Environment
- OCDE, 2021. Recommendation of the Council on Children in the Digital Environment. [online]. OECD. Disponible en: https://www.oecd.org/digital/ieconomy/protecting-children-online.htm https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- OCDE, 2021. Children in the digital environment revised typology of risks OECD digital economy papers January 2021 No. 302. En: https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1623292179&id=id&accname=guest&checksum=9AC7B897CADEB18BCD05055409C5ADFA
- OCDE, 2021. Innovation Blog. En: https://oecd-innovation-blog.com/2021/06/01/oecd-recommendation-children-digital-environment-online-safety-risks/
- OCDE, 2020, "Protecting children online: An overview of recent developments in legal frameworks and policies", *OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris.
- OCDE, 2019. Recommendation of the Council on Artificial Intelligence
- OCDE, 2017. Protection of Children Online: Preliminary Country Survey Findings and Proposal For Next Steps
- OCDE, 2013). Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

Parlamento Europeo (PE)

- El Parlamento Europeo, el Consejo y la Comisión (2023) Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01). Publicada el 23 de enero de 2023 en el Diario Oficial de la Unión Europea.
- Parlamento Europeo y Consejo (2016). Reglamento (UE) 2016/679 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).
- Parlamento Europeo, Consejo de la Unión Europea, Comisión Europea. 2000. Carta de los derechos fundamentales de la Unión Europea. El texto oficial fue publicado en el Diario Oficial de las Comunidades Europeas C 364/7 del 18 de diciembre de 2000.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Parlamento Latinoamericano y Caribeño (PLC)

- PLC, 2023. Ley Modelo de Neuroderechos para América Latina y el Caribe (Panamá 19 y 20 de mayo 2023)

Red Iberoamericana de protección de datos (RIPD)

- RIPD, 2024. Declaración sobre neurotecnologías y neurodatos en el marco de la normativa de protección de datos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en Cartagena, Colombia el 29 de mayo de 2024).
- RIPD, 2023. Declaración sobre neurodatos, aprobada en sesión cerrada del encuentro de la Red Iberoamericana de Protección de Datos, en la Antigua, Guatemala el 25 de septiembre de 2023.
- RIPD, 2019. Recomendaciones generales para el tratamiento de datos en la inteligencia artificial. México, junio de 2019
- RIPD, 2017. Estándares de protección de datos personales para los países Iberoamericanos

Secretaría General Iberoamericana (SEGIB)

Secretaría General Iberoamericana (2023) Carta Iberoamericana de Principios y Derechos en Entornos Digitales (CIPDED) aprobada durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, 25 de marzo de 2023.

Superintendencia de Industria y Comercio (SIC). Delegatura para la protección de datos personales

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- SIC, 2021. Guía cuida tu identidad digital y protege tus datos personales: riesgos sobre el tratamiento de datos personales de niños, niñas y adolescentes. En: https://www.sic.gov.co/sites/default/files/files/2021/Guia%20CUIDA%20TU%20IDENTIDAD%20DIGITAL%20002.pdf

Unión Europea (UE)

- UE (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)
- UE (2020). Estrategia Europea de Datos. En: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es
- UE (2016). Reglamento (UE) 2016/679 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).

Anexo 4. Principales normas constitucionales y legales sobre regulación de tratamiento de datos personales en los países miembros de la SEGIB

En el presente anexo se presenta la normativa vigente por país, distinguiendo fundamento constitucional y legislativo.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Andorra

- Constitución:
  - Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000
- Leyes:
  - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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)
  - Consell General d'Andorra. (2021). *Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals ;*

Argentina

- Constitución:
  - Artículo 43 de la Constitución de 1994
- Leyes:
  - Ley de Protección de Datos Personales N.º 25.326 de 2000
  - Reglamento de la ley datos Decreto N.º 1.558 de 2001.

Bolivia

- Constitución:
  - Artículos 21 y 130
- Leyes: No tiene ley de protección de datos.

Brasil

- Constitución:
  - Artículo 5 LXXII de la Constitución de 1998 y enmienda constitucional 115 de 2022
- Leyes:
  - Ley N.º 13.709/2018, Ley General de Protección de Datos Personales (LGPD)

Costa Rica

- Constitución:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- No

- Leyes:
  - Asamblea Legislativa de Costa Rica. Ley nº 8968, Protección de la Persona frente al tratamiento de sus datos personales. Diario Oficial La Gaceta, 7 de julio de 2011.
  - Poder Ejecutivo de Costa Rica. Decreto Ejecutivo No.37554-JP, Reglamento de la Ley nº 8968, 30 de octubre de 2012.
  - Poder Ejecutivo de Costa Rica. Directriz 046-H-MICITT, sobre computación en la nube en las instituciones públicas, 9 de abril de 2013.
  - Poder Ejecutivo de Costa Rica. Decreto Ejecutivo 40008, de reforma del Reglamento

Cuba

- Constitución:
  - Art 97 “Se reconoce el derecho de toda persona de acceder a sus datos personales en registros, archivos u otras bases de datos e información de carácter público, así como a interesar su no divulgación y obtener su debida corrección, rectificación, modificación, actualización o cancelación. El uso y tratamiento de estos datos se realiza de conformidad con lo establecido en la ley.”
- Leyes:
  - Gaceta Oficial de la República de Cuba, Ministerio de Justicia. "Ley 149/2022 'De Protección de Datos Personales'." Gaceta Oficial No. 90 Ordinaria (25 de agosto de 2022): GOC-2022-832-O90. Tomado de: https://www.gacetaoficial.gob.cu/sites/default/files/goc-2022-o90_0.pdf

Chile

- Constitución:
  - Constitución Política de la República de Chile, 1980 (última modificación en 2020). Artículo 19.4. "La Constitución asegura a todas las personas: (…) 4°. El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Esta versión fue incorporada al texto constitucional a través de la **ley N° 21.096**, titulada "Consagra el derecho a protección de los datos personales", publicada el 16 de junio de 2018, fecha en la que entró en vigor.

- Leyes:
  - Chile, Ley 21719 del 13 de diciembre de 2024 regula la protección y el tratamiento de datos personales y crea la agencia de protección de datos personales.
  - Chile, Ley 19628 Sobre Protección de la Vida Privada." Promulgada el 18 de agosto de 1999. Publicada el 28 de agosto de 1999. Última modificación el 10 de noviembre de 2022, Ley 21504. Última versión: 9 de mayo de 2023. Materias: Derecho a la Privacidad. http://www.bcn.cl/leychile/navegar?idNorma=141599
  - Chile, "Ley N° 19.812, que modifica la ley N° 19.628," publicada el 13 de junio de 2002.
  - Chile, "Ley N° 20.463, que modifica la ley Nº 19.628, suspendiendo por el plazo que indica la información comercial de las personas cesantes," publicada el 25 de octubre de 2010.
  - Chile, "Ley N° 20.521, que modifica la ley Nº 19.628, para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz," publicada el 23 de julio de 2011.
  - Chile, "Ley N° 20.575, que establece el principio de finalidad en el tratamiento de datos personales, modificando la ley N° 19.628," publicada el 17 de febrero de 2012.
  - Chile, "Ley N° 21.214, que modifica la ley N° 19.628, con el objeto de prohibir que se informe sobre las deudas contraídas para financiar la educación en cualquiera de sus niveles," publicada el 28 de febrero de 2020.
  - Chile, "Decreto Supremo N° 779/2000, del Ministerio de Justicia, que aprueba el Registro de Bancos de Datos Personales a Cargo de los Organismos Públicos," publicado el 11 de noviembre de 2000.
  -

Colombia

- Constitución:
  - Artículo 15 de la Constitución de 1991
- Leyes:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Ley Estatutaria 1581 de 2012
- Decreto 1377 de 2013 (Incorporado en el decreto 1074 de 2015)

Ecuador

- Constitución:
  - Constitución de la República del Ecuador. Decreto Legislativo. Registro Oficial 449, 20 de octubre de 2008. Art. 66. Numeral 19. El 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.
- Leyes:
  - Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459, 26 de mayo de 2021.

El Salvador

- Constitución: No
- Decreto 144 del 15 de noviembre de 2024, Ley para la protección de datos personales
- Leyes: Las siguientes son algunas leyes sectoriales o especiales
  - Ley de Protección al Consumidor (2005), que reconoce derechos a los consumidores frente a entidades especializadas en la prestación de servicios de información
  - Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas (2011), orientada a procurar, entre otras cosas, el buen manejo de los datos relativos al historial crediticio de consumidores o clientes
  - Ley de Acceso a la Información Pública (2011), que contiene todo un apartado relativo a la protección de datos, en el marco de la relación individuo-Estado
  - Ley Crecer Juntos (2022), que establece algunas regulaciones y prohibiciones sobre el tratamiento de datos de niñas, niños y adolescentes.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

España

- Constitución:
  - Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000.
  - Constitución Española. Publicada en el «BOE» núm. 311, de 29 de diciembre de 1978. Entrada en vigor el 29 de diciembre de 1978. Última actualización publicada el 17 de febrero de 2024. https://www.boe.es/eli/es/c/1978/12/27/(1)/con. Artículo 18. Numeral 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

- Leyes:
  - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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).
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Publicado en: «BOE» núm. 126, de 27/05/2021.

Guatemala

- Constitución:
  - Constitución Política de la República de Guatemala. 1985. Reformada en 1993. Artículo 24. - "Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna". Artículo 30. - "Publicidad de los actos administrativos." Artículo 31 . Acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos."

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Leyes: No tiene ley general de protección de datos

Honduras

- Constitución:
  - Artículo 31
- Leyes: No tiene ley general de protección de datos

México

- Constitución:
  - Artículos 6, 16 y 73 de la Constitución Política de los Estados Unidos Mexicanos 2008.
  - Decreto del 20 de diciembre de 2024 por el cual se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Mexicanos, en materia de simplificación orgánica.
- Leyes:
  - Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) del 5 de julio de 2010
  - Decreto por el cual se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Publicado el 5 de julio de 2017. En: https://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010#gsc.tab=0
  - Decreto por el cual se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Publicado el 26 de enero de 2017. En: https://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017#gsc.tab=0
  - Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Publicado el 21 de diciembre de 2011. En: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf
  - México ha suscrito el convenio 108 del 28 de enero de 1981 para la Protección de las Personas en cuanto al Tratamiento Automatizado de Datos de Carácter Personal.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Nicaragua

- Constitución:
  - Artículo 26.
- Leyes:
  - Nicaragua. Asamblea Nacional. *Ley de Protección de Datos Personales*, Ley No. 787, 21 de marzo de 2012. Publicada en *La Gaceta, Diario Oficial* N°. 61, 29 de marzo de 2012.
  - Nicaragua. Asamblea Nacional. *Reglamento de la Ley de Protección de Datos Personales*, Decreto No. 36-2012, 17 de octubre de 2012. Publicado en *La Gaceta, Diario Oficial* N°. 200, 19 de octubre de 2012.

Panamá

- Constitución:
  - Artículos 42 y 44
- Leyes:
  - Asamblea Nacional de Panamá, Ley 81 de 2019, "Sobre Protección de Datos Personales," Gaceta Oficial Digital (26 de marzo de 2019).
  -

Paraguay

- Constitución:
  - Convención Nacional Constituyente. Constitución de la República del Paraguay. Asunción, 20 de junio de 1992. Artículo 135. Habeas Data.
- Leyes: No tiene norma general de protección de datos. Cuenta con regulaciones especiales como, entre otras, las siguientes:
  - Congreso de la Nación Paraguaya. Ley 6534, De Protección de Datos Personales Crediticios. 27 de octubre de 2020
  - Congreso de la Nación Paraguaya. Ley Nº 3440. 16 de julio de 2008.
  - Congreso de la Nación Paraguaya. Ley Nº 4439. 3 de octubre de 2011.
  - Congreso de la Nación Paraguaya. Ley Nº 1682. 16 de enero de 2001.
  - Congreso de la Nación Paraguaya. Ley Nº 1969. 3 de septiembre de 2002.
  - Congreso de la Nación Paraguaya. Ley Nº 4017. 23 de diciembre de 2010.
  - Congreso de la Nación Paraguaya. Ley Nº 4610/2012.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- Presidencia de la República del Paraguay. Decreto Nº 7369. 23 de septiembre de 2011.
- Congreso de la Nación Paraguaya. Ley Nº 4868. 26 de febrero de 2013.
- Presidencia de la República del Paraguay. Decreto Nº 1165. 27 de enero de 2014.
- Congreso de la Nación Paraguaya. Ley Nº 4989. 9 de agosto de 2013.

Perú

- Constitución:
  - Congreso Constituyente Democrático. Constitución Política del Perú. Lima, 29 de diciembre de 1993. Artículos 2 y 200.
- Leyes:
  - Congreso de la República del Perú. Ley Nº 29733 de 2001 Protección de Datos Personales. 3 de julio de 2011.
  - Presidencia de la República del Perú. Decreto Supremo Nº 003-2013-JUS. 21 de marzo de 2013.
  - Presidencia de la República del Perú. Decreto legislativo Nº1353. 7 de enero de 2017.
  - Presidencia de la República del Perú. Decreto Supremo Nº 029-2021-PCM. 19 de febrero de 2021.
  - Presidencia de la República del Perú. Decreto supremo No. 016-2024-JUS del 30 de noviembre de 2024 que aprueba el reglamento de la Ley 29733, ley de protección de datos personales

Portugal

- Constitución
  - Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, aprobada el 7 de diciembre de 2000.
- Leyes:
  - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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)
  - Ley 58 de 2019

Con el apoyo de:
Con el apoyo de:
Cooperación Española

República Dominicana

- Constitución:
  - Constitución de la República Dominicana, proclamada el 26 de enero. Publicada en la Gaceta Oficial No. 10561, del 26 de enero de 2010. Artículo 44. Numeral 2. Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos;
  - Artículo 70. Hábeas data. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística
- Leyes:
  - Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. No. 10737 del 15 de diciembre de 2013.

Uruguay

- Constitución: No
- Leyes:
  - Ley de protección de datos personales N.º 18.331 del 18 de agosto de 2008
  - Decreto 414 del 31 de agosto de 2009 (Reglamenta la ley 18.331 de 2018)
  - Ley 19.670 de 2018 (Modifica parcialmente la ley 18.331 de 2018)

- Decreto 64 del 17 de febrero de 2020 (Reglamenta los artículos 37ª 40

Venezuela

- Constitución:
  - Constitución de la República Bolivariana de Venezuela. 1999. "Artículo 28 y Artículo 281, numeral 3.
- Leyes: No tiene norma general de protección de datos personales

Anexo 5. Proyectos de ley sobre Protección de Datos en la región Iberoamericana y otras iniciativas relevantes extra regionales.

Actualmente algunos países iberoamericanos están en proceso de expedir, por primera vez, una ley general sobre tratamiento de datos (Bolivia y Honduras). Otros, por su parte, han radicado proyectos de ley para modificar o actualizar sus regulaciones actuales (Argentina, Chile, Colombia, Costa Rica y República Dominicana).

Varios de ellos han tenido como referente los documentos internacionales mas recientes que mencionamos en este estudio. Lo anterior es muy importante para contar con regulaciones modernas y jurídicamente interoperables para, entre otros, afrontar los retos propios de una sociedad digital, global, transfronteriza que, en buena medida depende de los datos personales.

A continuación, nos referimos brevemente a los casos de Argentina, Bolivia, Chile, Colombia, Costa Rica, Honduras y República Dominicana:

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Argentina

El objetivo de este proyecto de ley es actualizar la Ley 25.326 de 2000 sobre protección de datos personales en Argentina. El gobierno argentino inició un proceso de revisión y modernización de la citada ley para dar respuesta a los desafíos tecnológicos y económicos actuales y armonizar con los estándares regionales e internacionales desde un enfoque de derechos humanos.

La Agencia de Acceso a la Información Pública inició un proceso de debate participativo, llevando a cabo mesas preparatorias y mesas de diálogo con diversos sectores de la sociedad durante los meses de julio y agosto de 2022. El 12 de septiembre de dicho año se abrió la consulta pública (Resolución AAIP 119/2022) para garantizar la participación efectiva de la ciudadanía, de acuerdo con el Reglamento General para la Elaboración Participativa de Normas

Como resultado, se presentó un Proyecto de Ley de Protección de Datos Personales[160]. El Poder Ejecutivo Nacional, con las firmas del Presidente de la Nación envió a la Honorable Cámara de Diputados de la Nación el Mensaje 87/2023 con el Proyecto de Ley.

El proyecto sigue en Cámara de Diputados ppara continuar el proceso legislativo respectivo.

[160][160] Referencias sobre el proyecto de ley de la República Argentina:

- Poder Ejecutivo Nacional. Proyecto de Ley 87/2023: Nueva Ley de Protección de Datos Personales. Enviado a la Honorable Cámara de Diputados de la Nación. Firmado por el Presidente Alberto Fernández y el Jefe de Gabinete Agustín Rossi. Presentado el 12 de septiembre de 2022. Accessed July 9, 2024. https://example.com/document.
- Argentina.gob.ar. "El objetivo es la actualización de la Ley 25.326 porque, si bien la Argentina fue precursora en la región en materia de Protección de Datos Personales, sentando…" Última modificación el 3 de julio de 2024. https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Bolivia

La AGECTIC[161] de Bolivia cuenta con un anteproyecto de Ley de Protección de Datos Personales del Estado Plurinacional de Bolivia (2023) que busca regular el citado derecho[162]. En el texto se destacan los siguientes aspectos :

- *Aplicación extraterritorial:* Regulación específica para responsables y encargados fuera de Bolivia que ofrezcan bienes o servicios a personas en Bolivia.
- *Ampliación de habilitantes:* Incluye habilitantes adicionales al consentimiento para tratar datos personales conforme al principio de licitud.
- *Principio de responsabilidad:* Enfatiza la necesidad de cumplir y demostrar el cumplimiento de los principios, facilitando la rendición de cuentas.
- *Principio de lealtad:* Prioriza los intereses de los titulares de datos y respeta su expectativa de privacidad.
- *Derechos de los titulares:* Reconoce derechos clásicos (acceso, rectificación, cancelación, oposición) e introduce derechos como portabilidad, limitación del tratamiento, y derecho a la información.
- *Transferencias internacionales:* Establece un régimen integral para transferencias internacionales, garantizando la protección de los titulares de datos.
- *Medidas preventivas (proactivas):* Incluye evaluaciones de impacto, privacidad desde el diseño y por defecto, y la figura del delegado de protección de datos.
- *Derecho a la indemnización:* Reconoce el derecho a la indemnización por daños y perjuicios causados por el tratamiento indebido de datos personales.

El texto subraya la importancia de la privacidad y protección de datos para la autodeterminación informativa en la era digital, considerando que su implementación puede impactar positivamente los derechos humanos, el desarrollo, la innovación y la democracia en Bolivia.

[161] Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC)
[162] Referencia sobre el anteproyecto de ley de Bolivia:
- Estado Plurinacional de Bolivia, Ministerio de la Presidencia, Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC). *Anteproyecto de Ley de Protección de Datos Personales*. 2023.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Colombia

En Colombia existen dos proyectos de ley relacionados con datos.

En primer lugar, el proyecto de ley Cámara 156/2023C "Por la cual se dictan disposiciones para el régimen general de protección de datos personales". Este busca actualizar la Ley Estatutaria 1581 de 2012 y propone una normativa exhaustiva para la protección y tratamiento de datos personales. Se trata de una propuesta de 108 artículos que crea un nuevo régimen general de tratamiento de datos y deroga la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa relacionada que sea contraria a las disposiciones del proyecto[163].

El texto fue retirado el 8 de mayo y se espera que prontamente se radique uno nuevo.

El proyecto fue presentado el 22 de agosto de 2023 y publicado en la Gaceta 1188 de 2023, con el objetivo de proteger los datos personales como un derecho fundamental, conforme a los artículos 15 y 20 de la Constitución colombiana[164]. El proyecto abarca tanto el tratamiento automatizado como no automatizado de datos, con excepciones claramente definidas, como las actividades personales y ciertos tratamientos realizados por autoridades competentes. Además, se extiende su aplicación territorialmente, vinculando la normativa al lugar de residencia del responsable del

[163] El texto del proyecto, los comentarios y debates sobre el mismo se puede consultar en: https://www.camara.gov.co/proteccion-de-datos-personales
[164] Referencia sobre el proyecto de ley de datos de Colombia:

- Proyecto de ley Cámara 156/2023C "Por la cual se dictan disposiciones para el régimen general de protección de datos personales" . Radicado el 22 de agosto de 2023 (Gaceta 1188 de 2023) . Mayor información sobre el proyecto y su trámite en el Congreso: https://www.camara.gov.co/proteccion-de-datos-personales

Con el apoyo de:
Con el apoyo de:
Cooperación Española

tratamiento y los titulares de los datos, así como a la oferta de bienes o servicios en el país, independientemente de su carácter oneroso.

Una de las innovaciones más destacadas es la regulación de los datos de personas fallecidas, estableciendo condiciones para que los herederos y las personas designadas puedan solicitar acceso, rectificación o supresión de estos datos. Además, se enfatiza la importancia del consentimiento demostrable y voluntario de los titulares de datos, con la posibilidad de revocarlo en cualquier momento.

En segundo lugar, en mayo de 2024, el Ministerio de Tecnologías de la Información y las Comunicaciones radicó el proyecto de ley **No. 447 de 2024** "Por medio de la cual se dictan disposiciones para el suministro, intercambio y aprovechamiento de la infraestructura de datos del Estado colombiano (IDEC) y la interoperabilidad de los sistemas de información de las entidades públicas"[165].

La iniciativa pone de presente algunas ideas del gobierno sobre el uso de información. Dicho proyecto tiene "por objeto establecer las disposiciones para el suministro, intercambio, y aprovechamiento de la infraestructura de datos del Estado colombiano (IDEC), la interoperabilidad de los sistemas de información de las entidades públicas y organismos, y la gobernanza, gestión y disponibilidad de los datos básicos, maestros, de referencia y abiertos del Estado colombiano, y con ello orientar la toma de decisiones del Gobierno Nacional y Territorial, que permitan mejorar la calidad de vida de los ciudadanos y el desarrollo de las actividades sociales y económicas del país"[166]

[165] Referencia sobre el proyecto de ley No. 447 de 2024:

- Colombia. Congreso de la República. Proyecto de Ley No. 447 de 2024 Cámara: Por medio de la cual se dictan disposiciones para el suministro, intercambio y aprovechamiento de la infraestructura de datos del Estado colombiano (IDEC) y la interoperabilidad de los sistemas de información de las entidades públicas. Bogotá, 2024.

[166] Cfr. Ministerio de Tecnologías de la Información y las Comunicaciones (2024). Artículo 1 del proyecto de ley "Por medio de la cual se dictan disposiciones para el suministro, intercambio y aprovechamiento de la infraestructura de datos del Estado colombiano (IDEC) y la interoperabilidad de los sistemas de información de las entidades públicas y se dictan otras disposiciones"

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Estas son las definiciones de los datos a que se refiere el artículo 3 proyecto de ley:

- "Dato maestro: Conjunto de datos centralizados, esenciales y transversales en una organización y que son definidos y establecidos como única fuente de verdad por esta. Pueden compartirse por diferentes sistemas de información de la organización o fuera de esta."
- "Dato referencia: Conjunto de datos proveniente de estándares internos o externos que permite la clasificación, la caracterización y la categorización de datos en la organización."
- "Datos básicos: Datos constituidos por los datos maestros, datos de referencia y datos abiertos y que son transversales y gestionados como única fuente de verdad para la ejecución de los procesos en organizaciones públicas y privadas. Son utilizados para el diseño de programas sociales, la investigación y el desarrollo social, económico y cultural"

La definición de dato abierto se encuentra en el literal j) del artículo 6 de la ley 1712 de 2014[167] en los siguientes términos: "j) Datos Abiertos. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos;"

El proyecto no modifica expresamente ninguna ley sobre tratamiento de datos y encarga de la vigilancia y control de la futura ley a "cada uno de los organismos del Estado que en el marco de sus competencias tenga que conocer de una o varias de las actividades involucradas en el proceso de suministro, intercambio, y aprovechamiento de la infraestructura de datos del Estado colombiano (IDEC), la interoperabilidad de los sistemas de información de las entidades públicas y organismos.".

[167] Cfr. Ley 1712 del 6 de marzo de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Adicionalmente, establece que "la Superintendencia de Industria y Comerio velará por el cumplimiento de las normas y leyes vigentes en relación con la protección de datos personales"[168]

En caso de convertise en ley, la misma es de obligatorio cumplimiento a las entidades públicas y a los particulares que cumplen funciones administrativas, públicas o que administren recursos del Estado[169]. Dichos sujetos estarían obligados a la garantizar la incorporación de los siguientes componentes para el suministro, intercambio y aprovechamiento de la infraestructura de datos del Estado y la interoperabilidad de los sistemas de información de las entidades públicas: " la estrategia y gobernanza de la infraestructura de datos del Estado; herramientas técnicas y tecnológicas; interoperabilidad de la infraestructura de datos; seguridad y privacidad de la infraestructura de datos; datos; y, aprovechamiento de datos." [170]. Adicionalmente, señala el proyecto que "todas las entidades cabeza de sector administrativo tendrán la obligación de implementar en coordinación con las entidades del sector, las recomendaciones, lineamientos y estrategias sectoriales expedidas por el Comité Nacional de Datos." [171].

El citado Comité Nacional de Datos será el responsable de la gestión y administración de los datos maestros y de referencia del país. La Agencia Nacional de Gobierno Digital – AND- ejercerá el rol de Secretaría Técnica[172].

[168] Cfr. Ministerio de Tecnologías de la Información y las Comunicaciones (2024). Artículo 29 del proyecto de ley
[169] Cfr. Ibid, artículo 2
[170] Cfr. Ibid, artículo 5
[171] Cfr. Ibíd., artículo 5"
[172] Cfr. Ibíd., artículo 18

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Costa Rica

La Ley N.º 8968, "Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales", vigente desde el 27 de junio de 2011 y publicada en la Gaceta N.º 170 el 5 de septiembre de 2011, constituye el marco legal actual para la protección de datos personales en Costa Rica. Sin embargo, se encuentra en proceso de derogación mediante el proyecto de ley N.º 23097, "Ley de Protección de Datos Personales", presentado el 9 de mayo de 2022 por varios diputados. Este proyecto fue dictaminado por la Comisión de Ciencia y Tecnología el 23 de enero de 2023[173].

El proyecto de ley N.º 23097 busca garantizar un tratamiento adecuado de los datos personales y elevar el nivel de protección de las personas físicas, independientemente de su nacionalidad. Su objetivo es asegurar el ejercicio y tutela efectiva del derecho a la protección de datos personales, facilitar el flujo internacional de datos y promover mecanismos de cooperación internacional. Los principios rectores de este proyecto incluyen exactitud, legitimación, lealtad, transparencia, limitación de la finalidad, minimización, responsabilidad proactiva, seguridad y confidencialidad. Además, el proyecto considera tratados internacionales, derecho comparado, principios y estándares internacionales, y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Honduras

Desde de abril de 2018 se debate en el Congreso Nacional de la República de Honduras un proyecto de Ley de Protección de Datos Personales[174]. Este proyecto es fundamental en la medida que Honduras no tiene una ley general sobre el tema.

[173] Referencia sobre el proyecto de ley de Costa Rica:

- Costa Rica. Asamblea Legislativa. *Proyecto de Ley N.º 23097, Ley de Protección de Datos Personales*. San José, 2022. https://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx.

[174] Referencia sobre el proyecto de ley de Honduras:

El proyecto resulta de la revisión de estándares internacionales en materia de protección de datos personales, incluyendo trabajos de la ONU, la Directiva 95/46/CE de la UE y propuestas de la Red Iberoamericana de Protección de Datos. Se complementa con un análisis comparativo de legislaciones referenciales de Colombia, Costa Rica, España, México, Uruguay y el Proyecto de Reglamento Comunitario de Protección de Datos de la UE. Este primer esfuerzo busca adaptar una legislación adecuada al contexto hondureño, abordando la protección de datos personales para garantizar la privacidad y el derecho a la autodeterminación informativa.

República Dominicana

En República Dominicana existe el proyecto de ley que modifica la Ley N.º 172-13 del 13 de diciembre de 2013 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

La amplia gama de derechos protegidos en la Constitución dominicana incluye la intimidad y el honor personal (artículo 44). El derecho a la protección de datos personales permite a cualquier persona acceder, actualizar, rectificar, oponerse y destruir sus datos en registros públicos o privados. El proyecto busca adecuarse a la sociedad de la información, garantizando la calidad, licitud, lealtad, seguridad y finalidad de los datos personales. Establece la creación de la Agencia Dominicana de Protección de Datos para velar por el cumplimiento de esta normativa y regular el manejo de datos personales en el país[175].

- Instituto de Acceso a la Información Pública (IAIP). Anteproyecto de Ley de Protección de Datos Personales de Honduras. https://cei.iaip.gob.hn/doc/Anteproyecto%20de%20Ley%20de%20Proteccion%20de%20Datos%20Personales%20y%20Accion%20de%20Habeas%20Data%20de%20Honduras%20%20Final%2021%2001%2014.pdf

[175] Referencia sobre el proyecto de ley de la República Dominicana.

Anexo 6: Identificación de buenas prácticas y experiencias comparadas en el tratamiento de datos personales.

"*Buenas prácticas*" comúnmente se refiere a experiencias que han producido resultados positivos, demostrando su eficacia y utilidad en un contexto concreto. Se trata de iniciativas exitosas dirigidas a mejorar lo que se hace para satisfacer las necesidades y expectativas de los clientes, los usuarios, terceros, etc. Tal y como lo anota el *International Bureau of Education* (IBE) de la UNESCO, definir el concepto de buena práctica no es fácil, pues este se utiliza en varios contextos. "*Se puede considerar que las "buenas prácticas" corresponden a casos en los cuales procesos y comportamientos han obtenido resultados positivos, es decir, que las "buenas prácticas" son comparables a las "mejores prácticas"*. Otros definen una "buena práctica" de manera más general, "*considerándola como un enfoque que frecuentemente es innovador, que ha sido probado y evaluado y que tiende a tener éxito en otros contextos. Una buena práctica es la innovación que permite mejorar el presente y por lo tanto es o puede ser un modelo o norma para determinado sistema*"[176] . Señala Beatriz Boza que una buena práctica es "*una actividad o proceso que ha producido destacados resultados en el*

- Proyecto de ley que modifica la Ley N.º 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Santo Domingo, 2023. https://www.senado.gov.do/wfilemaster/lista_expedientes.aspx?coleccion=53

[176] Cita traducida de : "Conceptualisation et dissémination des bonnes pratiques en éducation: essai d'une approche internationale à partir d'enseignement tirés d'un projet", Abdoulaye Anne, en "Développement curriculaire et "bonne pratique" en éducation". 2003, PDF 324 KB (en francés).

manejo de una organización y que puede ser replicada en otras organizaciones para mejorar la efectividad, eficiencia e innovación de las mismas"[177].

En Europa, países como Andorra y España muestran un nivel avanzado de implementación. Andorra, por ejemplo, ha desarrollado una serie de guías detalladas que abarcan diversos aspectos de la protección de datos. Su "Guía informativa de Evaluación de Impacto en Protección de Datos" (2023) proporciona una metodología para identificar y controlar riesgos asociados al tratamiento de datos personales. Complementariamente, la "Guía de buenas prácticas del deber de información" (2022) ofrece orientaciones específicas para cumplir con la obligación de informar a los titulares de datos. Estas guías demuestran un enfoque proactivo y preventivo, alineado con principios internacionales de privacidad por diseño y por defecto (Agencia Andorrana de protección de datos, 2022, 2023).

España, por su parte, destaca por tener un amplio compilado de guías prácticas, incluyendo una "Guía de buenas prácticas en materia de Transparencia y Protección de Datos". Este documento refleja el esfuerzo por equilibrar la transparencia gubernamental con la protección de la privacidad, un desafío común en la era digital (Crue Universidades Españolas, s.f.). La "Guía para una Evaluación de Impacto en la Protección de Datos Personales" (2014) de España también demuestra una adopción temprana de prácticas que luego se volverían estándar en la Unión Europea con el GDPR.

En Centroamérica, se observan esfuerzos por desarrollar guías ciudadanas y mecanismos de acceso a datos, aunque con un nivel de implementación menos avanzado que en Europa. Costa Rica, por ejemplo, cuenta con una "Guía práctica de protección de datos para ayuntamientos" (Davara y Davara Asesores Jurídicos, 2006), lo que sugiere un enfoque en la implementación a nivel local. El Salvador ha desarrollado una "Guía para la implementación de una política pública de protección de datos" (IPANDETEC Centroamérica, 2021), indicando un esfuerzo por establecer un marco nacional coherente.

Es notable el uso de medios audiovisuales para la educación ciudadana en esta región. El Salvador, por ejemplo, ha producido un video educativo sobre el derecho de acceso a la información pública (Instituto de Acceso a la Información Pública, 2020). Panamá también ha desarrollado videos sobre

[177] Boza, Beatriz. *Acceso a la información del Estado: marco legal y buenas prácticas*. Konrad Adenauer Stiftung. Página 71. Lima, Perú. 2004.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Guías de Protección de Datos Personales. Estos esfuerzos sugieren un reconocimiento de la necesidad de hacer accesible la información sobre protección de datos a un público más amplio.

En Suramérica, países como Argentina, Brasil, Chile y Perú muestran un desarrollo más avanzado en comparación con otros de la región. Argentina ha elaborado una "Guía de Evaluación de Impacto en la Protección de Datos" y "Lineamientos para la formulación de un Plan de Protección de Datos Personales" (Consejo Federal para la Transparencia, 2023), lo que indica un enfoque en la planificación estratégica y la evaluación de riesgos.

Brasil ha desarrollado guías orientativas específicas, como la de "Tratamiento de datos personales por el Poder Público" y la "Aplicación de la LGPD en el contexto electoral" (Autoridad Nacional de Protección de Datos, 2022). Estas guías reflejan una consideración de los desafíos particulares en el sector público y en contextos políticos sensibles.

Chile ha realizado estudios de transparencia y cuenta con una "Guía para el resguardo de datos personales en plataformas de datos abiertos" (Consejo para la Transparencia, s.f.), lo que sugiere un enfoque en la intersección entre transparencia gubernamental y protección de datos. Su estrategia 'Chile Digital 2035' también enfatiza la necesidad de una robusta estrategia de ciberseguridad, vinculando la protección de datos con la seguridad digital más amplia (Biblioteca del Congreso Nacional de Chile, 2023).

Perú ha desarrollado un "Manual de protección de datos personales" (Defensoría del Pueblo, 2019) y una guía para oficiales de protección de datos (Autoridad Nacional de Protección de Datos Personales, 2023), lo que indica un enfoque tanto en la educación ciudadana como en la profesionalización de la protección de datos. También han producido un video educativo sobre el derecho a la protección de datos personales, siguiendo la tendencia regional de utilizar medios audiovisuales para la educación ciudadana.

Uruguay destaca por su "Guía Criterios de Disociación de Datos Personales" (2017), que aborda específicamente la anonimización de datos, un tema crucial en la era de los datos abiertos y el big data. También han desarrollado guías para la inscripción de bases de datos y sobre el rol del Delegado de Protección de Datos, lo que sugiere un enfoque integral que abarca aspectos técnicos, administrativos y de gobernanza.

Es importante notar que algunos países como Cuba, República Dominicana, Ecuador, Honduras, Nicaragua y Venezuela no presentan información sobre buenas prácticas en protección de datos

Con el apoyo de:
Con el apoyo de:
Cooperación Española

personales, lo que sugiere un área de oportunidad para el desarrollo de estas prácticas en dichos países.

En conclusión, se observa una tendencia general hacia la implementación de buenas prácticas en protección de datos personales en la mayoría de los países analizados, con un enfoque principal en el desarrollo de guías y capacitaciones. Sin embargo, el nivel de implementación varía significativamente entre regiones y países. Europa muestra un nivel más avanzado y comprensivo, mientras que en América Latina se observan esfuerzos significativos pero dispares, con algunos países liderando el camino y otros aún en etapas iniciales. El uso creciente de medios audiovisuales para la educación ciudadana es una tendencia positiva que podría facilitar una mayor comprensión y adopción de prácticas de protección de datos. La ausencia de información en algunos países sugiere la necesidad de un mayor desarrollo y posiblemente de cooperación internacional en esta área.

A la fecha se han identificado las siguientes buenas prácticas:

Creación de canales prioritarios para casos especiales o para la protección de los datos personales de las niñas, los niños y los adolescentes (NNA).

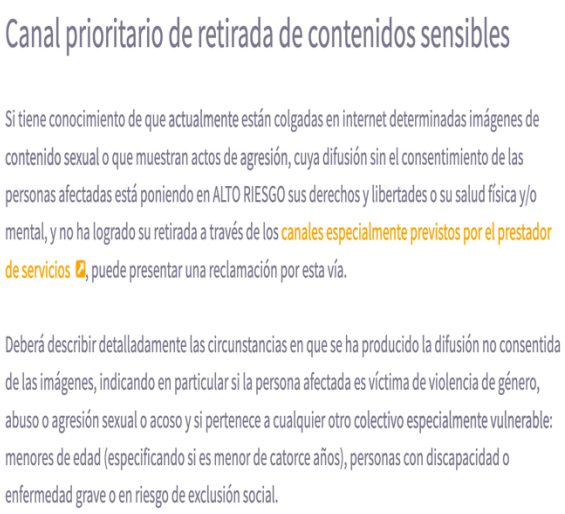
Esto puede contribuir a superar las dificultades en el ejercicio de los derechos de los NNA. Según un informe reciente, “los niños no comprenden plenamente sus derechos, carecen de competencias de alfabetización digital y pueden ser objeto de influencias indebidas” [178]

[178] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 15

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Destacamos la labor de la AEPD[179] en la creación del siguiente canal prioritario: https://www.aepd.es/canalprioritario

Fuente: AEPD, https://www.aepd.es/canalprioritario (Última consulta: 28/VII/2024)



Fuente: AEPD, https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/nuevaReclamacion.jsf?QID=Q600&ce=0 (Última consulta: 28/VII/2024)

Según la AEPD, el canal prioritario "se ha habilitado para la atención de **situaciones excepcionalmente delicadas**, cuando los contenidos (fotografías o vídeos) tengan **carácter sexual** o

[179] https://www.tudecideseninternet.es/

muestren actos de **agresión** y se estén poniendo en **alto riesgo** los derechos y libertades de los afectados, siempre que éstos sean personas españolas o se encuentren en España, especialmente si se trata de **menores de edad** o de **víctimas de violencia por razón de género**. Pueden acudir a este canal tanto el afectado como cualquier persona que tenga conocimiento de la difusión de este tipo de contenidos. (…) Podrás acudir a este canal sólo en casos excepcionales en los que, por tratarse de datos especialmente sensibles, la privacidad de la persona afectada se esté poniendo en grave peligro."[180]

Según información difudida por la AEPD en la red social X, "En 2023 la Agencia realizó 36 intervenciones de urgencia a través del Canal Prioritario para solicitar la retirada de contenido sexual o violento publicado en Internet sin consentimiento. El porcentaje de efectividad en la retirada es del 100%."

Promover la sensibilización sobre la protección de datos entre los NNA

La Comisión Europea, por ejemplo, en el marco de la estrategia para una internet mejor para los niños, ha venido proporcionando a los niños recursos de sensibilización y formación sobre sus derechos digitales, especialmente la protección de datos (por ejemplo, el consentimiento digital). [181]

Continuar educando a la población sobre el derecho de protección de datos

[180] Cfr. AEPD. ¿En qué casos puedo acudir a este canal?. https://www.aepd.es/preguntas-frecuentes/15-difusion-ilegitima-contenidos-sensibles/FAQ-1502-en-que-casos-puedo-acudir-a-este-canal (Última consulta: 28/VII/2024)
[181] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 15

Si bien se ha avanzado en la difusión del derecho a la protección de datos. Aún es un tema no conocido por todas las personas. Ese desconocimiento puede ser un factor para que las personas no ejerzan sus derechos o que, adopten medidas para ser los principales protectores del mismo. Dado lo anterior, se ha señalado que "las autoridades de protección de datos dedican recursos sustanciales a promover el conocimiento sobre los derechos y las obligaciones en materia de protección de datos entre el público en general, por ejemplo, a través de las redes sociales y campañas de televisión, líneas de ayuda, boletines informativos y presentaciones en las instituciones educativas". [182]

Facilitar herramientas para facilitar y demostrar cumplimiento de la regulación sobre tratamiento de datos

Proporcionar a los Resposables y Encargadosun conjunto de instrumentos que le permitan a las organizaciones facilitR Y demostrar de manera flexible y sencilla el cumplimiento de regulación como,entre otros:

- Códigos de conducta: "Las empresas subrayan que los códigos de conducta tienen un gran potencial como instrumento de cumplimiento debido a su especificidad por sectores y a su rentabilidad" [183]
- Mecanismos de certificación
- Modelos de clásulas contractuales: "proporcionan una herramienta de cumplimiento voluntaria prediseñada y fácil de aplicar que resulta especialmente útil para las pymes u

[182] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 13
[183] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 16

organizaciones que pueden no disponer de los recursos necesarios para negociar contratos individuales con sus socios comerciales." [184]

Ayuda a las pymes para cumplir la regulación

Usualmente, muchas pymes no cuentas con recursos, ni disponen de personal experto en protección de datos. Según la Comisión Europea (CE) "las pymes de muchos Estados miembros subrayan los beneficios de un apoyo personalizado por parte de sus autoridades locales de protección de datos". Por eso, según la CE, "las autoridades de protección de datos deben redoblar sus esfuerzos para hacer frente a estos desafíos, en particular mediante la colaboración proactiva con las pymes para disipar las preocupaciones infundadas en lo que respecta al cumplimiento" [185].

Con miras a logar lo anterior se puede acudir mecanismos sencillos mediante los cuales se brinde ayuda fácilmente comprensible a cualquier persona no experta en protección de datos personales como, entre otros:

- Usar herramientas prácticas, como plantillas o modelos (por ejemplo, para realizar evaluaciones del impacto derivado de la protección de datos).
- Crear líneas telefónicas o canales de ayuda
- Proporcionar ejemplos ilustrativos, listas de comprobación o chequeo y orientaciones sobre operaciones de tratamiento específicas y medidas técnicas y organizativas.

[184] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 16
[185] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 17

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Crear herramientas digitales para el ejercicio de los derechos ante los responsables del tratamiento y la autoridades de protección de datos

También se ha constatado que las autoridades de protección de datos "han desarrollado varias herramientas digitales de uso sencillo para facilitar a los interesados el ejercicio de sus derechos". [186].

Esta práctica genera los siguientes beneficios:

- Promueve que las personas exijan la protección de sus derechos de manera correcta
- Evita que las personas presenten solicitudes incompletas o infundadas que: (i) no permiten protección del derecho o (ii) generen que el proceso demande mayor tiempo para adoptar una decisión debido a los errores u omisiones en la presentación de la queja o recurso.
- Ayuda a las personas a conocer qué puede y qué pueden exigir en torno al derecho a la protección de datos

Creación de mecanismos voluntarios y alternativos de solución de controversias sobre tratamiento de datos (experiencia del caso SICFACILITA de la República de Colombia)

Usualmente, la protección de los derechos de los titulares de los datos ha estado centrada en la labor que realizan las autoridades de protección de datos de cada país. Aunque han realizado esfuerzos importantes, es sabido que les es imposible garantizar este derecho a todas las personas por varias razones como, entre otras, las siguientes:

a) La falta de recursos económicos y humanos para cumplir adecuadamente sus funciones.

[186] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 13

b) El incremento significativo de quejas ciudadanas que genera que se congestionen las autoridades de protección de datos, lo cual les impide dar las respuestas efectivas y oportunas que esperan las personas afectadas por el indebido tratamiento de sus datos personales.

Dado lo anterior, es necesario que las personas cuenten con otras alternativas de soluciones de controversias sobre tratamiento de datos, que sean complementarias a las acciones judiciales o administrativas actualmente existentes. Se trata de ampliar el abanico de opciones con el que puede contar el titular del dato para exigir el debido tratamiento de sus datos personales.

En el caso de la República de Colombia, se creó SICFACILITA como una herramienta gratuita de resolución de conflictos sobre, entre otros, tratamiento de datos personales creada por la Superintendencia de Industria y Comercio (SIC) de la República de Colombia.[187]

Quienes deseen usar libremente SICFACILITA (Responsables y Titulares de los datos) se reunen a través de un chat administrado por la SIC, con el objetivo de resolver problemas relacionados con tratamiento de datos personales. La idea es lograr una solución más expedita y eficaz sin necesidad

[187] Cfr. Qué es SIC Facilita. En: https://sicfacilita.sic.gov.co/SICFacilita/index.xhtml

Con el apoyo de:
Con el apoyo de:
Cooperación Española

de acudir a una actuación administrativa ante la autoridad de datos o una acción judicial. En suma, mediante SICFACILITA se acude a herramientas tecnológicas sencillas y de fácil acceso para buscar soluciones rápidas y efectivas frente a otras existentes actualmente.

En febrero de 2019, la autoridad colombiana de protección de datos (Delegatura de protección de datos de la SIC) creo y puso en marcha estas alternativas de solución de controversias sobre protección de dato personales. Los resultados han sido positivos. En marzo de 2022, por ejemplo, se destacó lo siguiente: "*En febrero de 2019 se puso en manos de los ciudadanos la herramienta SICFACILITA. Ese mecanismo ha demostrado ser útil para el ciudadano (Titular del dato) ya que ha servido para solucionar positivamente el 76,7% de las 9635 solicitudes ciudadanas. Adicionalmente, el tiempo de respuesta para solucionar cada caso es de 20 días en promedio.* ***En suma, SICFACILITA para datos personales ha sido un mecanismo rápido y efectivo de solución de conflictos para exigir el respeto de los derechos de los titulares de los datos personales***."[188] (Destacamos)

Nótese la rapidez de la respuesta para solucionar el caso (en promedio 20 días). Ese término es muy corto frente al que se demoraría iniciar una acción administrativa ante la autoridad de datos personales (en promedio 6 meses). También es destacable el nivel de efectividad (76.7%) porque eso significa que 7390 personas obtuvieron respuesta positiva y pronta frente a la vulneración de sus derechos.

Luego de 5 años de uso de SICFACILITA las cifras sigen siendo positivas. Desde febrero de 2019 al 31 de marzo de 2023 se recibieron 19.441 reclamaciones. De ellas, 14,669 (75,45%) llegaron a un

[188] República de Colombia. Superintendencia de Industria y Comercio. Delegatura de Protección de Datos. Oficio 22-127697- -0-0 del 31 de marzo de 2022 (informe de gestión desde el 23 de octubre de 2018 hasta el 31 de marzo de 2022). Páginas 5-6.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

acuerdo o solución expedita[189]. La mayor pretensión o solicitud de los ciudadanos es la eliminación de reportes negativos ante centrales de riesgo (16,107 solicitudes de eliminación, equivalentes al 82,9%)[190].

En conclusión, las alternativas de resolución de controversias en materia de tratamiento de datos personales como SICFACILITA, han mostrado ser útiles, expeditas y eficientes para proteger los derechos de los titulares de los datos. Adicionalmente, el uso de dichos mecanismos ayuda a disminuir el número de quejas ciudadanas frentes a las autoridades de protección de datos. Con ello se evita que dichas organizaciones se hiper congestionen y que, por ende, los tiempos de respuesta frente a las solicitudes de los titulares de los datos sean mucho mayores que los actuales.

De los países miembros de la SEGIB resaltamos la siguiente información sobre buenas prácticas:

1. Andorra

1.1. **Guía ciudadana:** Agencia Andorrana de protección de datos. Guia informativa de l'Avaluació d'Impacte en Protecció de Dades (AI) (2023)

[189] Cfr. República de Colombia. Superintendencia de Industria y Comercio.Informe SIC FACILITA del Grupo de Trabajo de atención al ciudadano (módulo de protección de datos personales -habeas data-). Página 1. Diciembre 31 de 2023. Páginas 5-6.

[190] Cfr. República de Colombia. Superintendencia de Industria y Comercio.Informe SIC FACILITA del Grupo de Trabajo de atención al ciudadano (módulo de protección de datos personales -habeas data-). Página 1. Diciembre 31 de 2023. Páginas 5-6.

https://www.apda.ad/storage/helps/fUCPtAfCs3M44wkQGA9ug4XEUWhRuvtCyMVXnkdJ.pdf En el presente documento se muestra una guía para la construcción de Evaluación de impacto sobre la normativa de protección de datos en Andorra. Busca identificar y controlar los riesgos para los derechos y libertades de las personas, asociados a un tratamiento de datos.

1.2. Autoridad Andorrana de Protección de Datos. *Guía de buenas prácticas del deber de información*. November 16, 2022. https://www.apda.ad/storage/guides/980PhG8cI2pcJZDefdQEx3yA09XwsSfjldvaopQT.pdf. Esta guía va dirigida a los responsables de tratamiento a quienes resulte aplicable la Ley 29/2021, de 28 de octubre, calificada de protección de datos personales (LQPD), así como a los profesionales que contribuyen, ya sea dentro de sus organizaciones o como encargados de tratamiento, en las tareas de asesorar a los responsables de tratamiento respecto de las obligaciones que les incumben en virtud de la LQPD. El deber de informar se encuentra recogido en los artículos 16 y 17 de la LQPD y representa la forma con la que se da cumplimiento al principio de transparencia. El **objetivo** de la guía es orientar en torno a las mejores prácticas para el cumplimiento del deber de informar a los interesados (titulares de los datos personales - personas físicas identificadas o identificables a las que corresponden los datos de carácter personal objeto de tratamiento) sobre todo lo relacionado con las circunstancias y condiciones del tratamiento de sus datos personales, así como de los derechos que les asisten. Esta guía cubre únicamente este objetivo específico y debe complementarse con otras guías en relación a la aplicación de la LQPD. En consecuencia, procedimientos, modelos, formularios, cláusulas, etc. habrán de ser revisados y adaptados por los responsables de tratamientos con anterioridad a la fecha de plena aplicación de la LQPD, incorporando los nuevos requisitos de acuerdo con las orientaciones que se proporcionan en esta guía.

1.3. Autoridad Andorrana de Protección de Datos. *Guía práctica para saber si mi entidad debe designar un Delegado de Protección de Datos (DPD)*. May 11, 2022. https://www.apda.ad/.

1.4. Autoridad Andorrana de Protección de Datos. *Guía sobre el uso de Cookies, política de privacidad y aviso legal*. March 30, 2022.

1.5. Autoridad Andorrana de Protección de Datos. *Guía informativa sobre la figura del Delegado de Protección de Datos (DPD)*. March 7, 2022.

2. Argentina

2.1. **Guía ciudadana:** *Guía de Evaluación de Impacto en la Protección de Datos (s.f)* https://www.argentina.gob.ar/sites/default/files/guia_final.pdf El documento aborda la importancia del derecho a la privacidad y la protección de datos personales, presentando conceptos fundamentales y explicando la Evaluación de Impacto en la Protección de Datos (EIPD). Además, detalla la metodología para la elaboración de la EIPD, incluyendo la determinación de participantes, análisis normativo, gestión de riesgos y las etapas posteriores, como la elaboración del informe final y la ejecución del plan de acción.

2.2. **Plan de trabajo:** Consejo Federal para la Transparencia (2023), Lineamientos para la formulación de un Plan de Protección de Datos Personales. Buenos Aires: Agencia de Acceso a la Información Pública.: El Consejo Federal para la Transparencia (CFT), creado por la Ley 27.275 de Acceso a la Información Pública, coordina políticas de transparencia y protección de datos personales entre las distintas jurisdicciones de Argentina, contando con apoyo de la Agencia de Acceso a la Información Pública. En 2023, la Comisión de Gobernanza de Datos y Protección de la Privacidad del CFT se enfocó en la creación de un Plan de Protección de Datos Personales para el sector público, destacando la importancia del tratamiento responsable de datos personales en la mejora de servicios y políticas públicas, y la necesidad de abordar los riesgos asociados.

2.3. **Modelo de política:** Recomendación a los organismos públicos titulares de bases de datos personales sobre la implementación de una política de protección de datos personales, y su difusión en forma permanente y actualizada https://www.argentina.gob.ar/aaip/datospersonales/politica-modelo-organismos-publicos

3. Bolivia

3.1. **Guía ciudadana:** En abril, Access Now y Fundación Internet Bolivia publicaron una guía sobre Protección de Datos Personales en Bolivia, que incluye definiciones básicas y el marco legal actual. La guía destaca la importancia de la protección de datos como un componente esencial de los derechos humanos en el uso de la tecnología y detalla conceptos como los tipos de datos personales, derechos de los titulares y la situación legal en Bolivia, donde aún no existe una legislación general sobre el tema, subrayando la necesidad de una ley integral que unifique las diversas disposiciones sectoriales existentes. https://www.accessnow.org/wp-content/uploads/2019/03/Guia-Basica-Proteccion-de-Datos-Bolivia.pdf y Céspedes Sagardía, Diandra Nathaly, Wilfredo Jordán, Tania Oroz, Diandra

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Céspedes, Carlos Guerrero, Jorge Nava, Mariana Ottich, y Esther Mamani. *Guía de Soluciones Legislativas para la Protección de Datos Personales*. Revisión por Cristian León. Diagramación por Marcelo Lazarte. Fundación Internet Bolivia, 2021. (https://internetbolivia.org/file/2021/11/guia_soluciones_legislativas.pdf)

4. Brasil:

4.1. **Guía e informe:** Bioni, Bruno, y Rafael Zanatta, dirs. *Informe Anual 2020 Data Privacy Research*. 2020. "A pesar de estas tremendas victorias, especialmente la aprobación de la LGPD, todavía estamos arrastrándonos en el proceso de formación de una cultura de protección de datos. Todavía queda mucho camino por recorrer para que la privacidad sea un pilar de la democracia brasileña y de la economía digital que se está construyendo en el país.

4.2. **Guía: Tratamento de dados pessoais pelo Poder Público guia orientativo** versão 2.0 junio 2023 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf Autoridad Nacional de Protección de Datos (ANPD). *Guia Orientativo: Tratamento de dados pessoais pelo Poder Público*. 2022 Considerando estas cuestiones, el presente *Guía Orientativa* busca delinear parámetros que puedan ayudar a entidades y organismos públicos en las actividades de adecuación e implementación de la LGPD. Las orientaciones presentadas constituyen un primer paso en el proceso de delimitación de las interpretaciones sobre la LGPD aplicables al Poder Público. Por eso, la versión publicada estará abierta a comentarios y contribuciones de manera continua, con el fin de actualizar la guía oportunamente, a medida que se establezcan nuevas reglamentaciones y entendimientos, a criterio de la ANPD. Las sugerencias pueden enviarse a la Ouvidoría de la ANPD, a través de la Plataforma Fala.BR (https://falabr.cgu.gov.br/). Cabe destacar que esta guía no tiene como objeto la definición de los conceptos básicos previstos en la LGPD. En caso de duda, se sugiere consultar la página de documentos y publicaciones de la ANPD, donde están disponibles orientaciones más específicas sobre estos conceptos, como el *Guía Orientativa para Definiciones de los Agentes de Tratamiento de Datos Personales y del Encargado*.

4.2.1. La guía comienza con una breve explicación sobre la LGPD, el concepto de Poder Público y las competencias de la ANPD. Luego, se presentan orientaciones sobre las bases legales más comunes y los principios más relevantes que deben guiar el tratamiento de datos personales por

Con el apoyo de:
Con el apoyo de:
Cooperación Española

entidades y organismos públicos. En la parte final, se abordan dos operaciones específicas de tratamiento de datos personales por el Poder Público: el intercambio y la divulgación de datos personales, siempre bajo el enfoque de la conformidad del tratamiento con la LGPD. Los Anexos I y II incluyen, respectivamente, un resumen de las recomendaciones presentadas en el análisis de los dos casos específicos mencionados.

4.3. **Guía**: Autoridad Nacional de Protección de Datos (ANPD). *Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. 2022. El propósito de esta guía es, a partir de una lectura sistemática de las normas de protección de datos personales y de las normas electorales, presentar los principales aspectos a ser considerados por candidatos, coaliciones, federaciones y partidos políticos para el tratamiento de datos personales de los titulares, electores o electores potenciales. Las orientaciones de esta publicación buscan garantizar la protección de datos, la privacidad de los titulares y la integridad del proceso electoral, sin obstruir la comunicación entre candidato y ciudadano, necesaria para el proceso democrático.

4.4. **Guía**: Más ciudadana, menos técnica. Núcleo de Protección de Datos del Consejo Nacional de Defensa del Consumidor, en asociación con la Autoridad Nacional de Protección de Datos y la Secretaria Nacional del Consumidor de Brasil. *Cómo Proteger sus Datos Personales: Guía*. 2022.

5. Colombia

Nos remitimos a lo señalado sobre SIC-facilita como alternativa de resolución de controversias.

6. Costa Rica:

6.1. **Guia ciudadana:** Davara y Davara Asesores Jurídicos. (2006). Guía práctica de protección de datos para ayuntamientos. Editorial: Wolters Kluwer España S.A.
Instrucción clara sobre mecanismo para acceder a datos: De acuerdo con el artículo 7 de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (n.º 8968) de Costa Rica, tiene el derecho de solicitar la rectificación de sus datos personales publicados en la web o en resoluciones judiciales. Para realizar esta solicitud, debe enviar los datos requeridos al correo electrónico.

(https://salaprimera.poder-judicial.go.cr/index.php/component/content/article/204-proteccion-de-datos?Itemid=223)

7. **Cuba**: No se encontró información pública al respecto.

8. **Chile**:

8.1. **Estudio de transparencia:** El estudio del Consejo para la Transparencia de Chile (2019) examina la percepción y el estado de la protección de datos personales en el país. Destaca el impacto de la economía digital y la digitalización en la acumulación masiva de datos, que ahora se generan a un ritmo alarmante. Esta realidad conlleva oportunidades pero también riesgos significativos, con problemas notorios como las filtraciones de datos en Facebook y Google+. Aunque Chile fue pionero en 1999 con una legislación de protección de datos, la Ley N° 19.880 se ha quedado obsoleta. Actualmente, se debate un nuevo proyecto de ley en el Congreso que propone modernizar la regulación siguiendo el modelo del GDPR europeo. Este proyecto busca introducir nuevos derechos, medidas de seguridad, un sistema de control efectivo y una autoridad independiente para garantizar el cumplimiento. (https://www.consejotransparencia.cl/wp-content/uploads/2020/02/Estudio-NT2019_Percepci%C3%B3n-Protecci%C3%B3n-de-Datos-Personales.pdf)

8.2. "Estudio analiza la protección de datos personales en Chile: ¿En qué nivel se encuentra y qué falencias existen?" *Protec Data*, 2024. https://protecdatalatam.com/blog/estudio-analiza-la-proteccion-de-datos-personales-en-chile-en-que-nivel-se-encuentra-y-que-falencias-existen/.

8.3. **Guía ciudadana:** Guía para el resguardo de los Datos Personales en el desarrollo e implementación de Plataformas de Datos Abiertos por parte de los órganos de la Administración del Estado: “El Consejo para la Transparencia da a conocer 11 directrices que orientarán a los organismos públicos en el diseño e implementación de Portales de Datos Abiertos, desde la perspectiva de la debida protección de los datos personales. Las directrices que se presentan a continuación dan cuenta de un enfoque proactivo y pre-ventivo, y se elaboraron sobre la base de los principios de privacidad por defecto y por diseño, así como en la necesidad de emplear técnicas y herramientas que permitan la debida anonimización de los datos perso-nales que puedan formar parte de las bases o bancos de datos que se pretende disponibilizar como datos abiertos, evitando cualquier vulneración respecto de los derechos que

Con el apoyo de:
Con el apoyo de:
Cooperación Española

la Constitución y la Ley N°19.628, recono-cen a sus titulares" (https://www.consejotransparencia.cl/guia-para-el-resguardo-de-los-datos-personales-en-el-desarrollo-e-implementacion-de-plataformas-de-datos-abiertos-por-parte-de-los-organos-de-la-administracion-del-estado/)

8.4. **Guía ciudadana:** El informe "Chile Digital 2035" enfatiza la necesidad de una robusta estrategia de ciberseguridad para avanzar en la transformación digital. La Mesa de Ciberseguridad ha proporcionado aportes para desarrollar estrategias holísticas que aborden las vulnerabilidades y necesidades del país. Desde la implementación de la Política Nacional de Ciberseguridad (2017-2022) hasta la promulgación de la Ley N° 21.459, que actualiza la normativa sobre delitos informáticos, Chile ha dado pasos significativos en esta área. Además, se están elaborando legislaciones marco para ciberseguridad y protección de datos personales. La academia también juega un papel crucial al formar nuevos profesionales y promover la ciberhigiene. A pesar de los avances, eventos recientes subrayan la continua vulnerabilidad del país, aunque también reflejan un creciente reconocimiento de la importancia de la ciberseguridad. Estrategia 'Chile Digital 2035': Construyendo la Ciberseguridad en Chile." Biblioteca del Congreso Nacional de Chile, 2023. https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/89176/3/Construyendo_la_Ciberseguridad_en_Chile.pdf.

9. R. Dominicana: No se encontró información pública al respecto.

10. Ecuador: No se encontró información pública al respecto.

11. El Salvador

11.1. **Guía ciudadana:** Guía para la implementación de una política pública de protección de datos (2021) IPANDETEC Centroamérica es una organización sin fines de lucro, basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica. https://www.ipandetec.org/wp-content/uploads/2021/06/SALVADOR.pdf

11.2. **Video educativo:** Campaña del Instituto de Acceso a la Información Pública sobre el derecho de acceso a la información pública. Noviembre 2020 https://www.youtube.com/watch?v=lLEtbihn3Ss

12. España:

12.1. **Guías: Compilado de guías** https://www.aepd.es/guias-y-herramientas/guias https://dpd.ua.es/es/guias-de-la-agencia-espanola-de-proteccion-de-datos.html

12.2. **Guía de buenas prácticas en materia de Transparencia y Protección de Datos:** https://www.crue.org/wp-content/uploads/2020/02/Gui%CC%81a-de-buenas-pra%CC%81cticas_VD.pdf

12.3. GUÍA para una Evaluación de Impacto en la de Protección Datos Personales (2014) https://icoec.es/wp-content/uploads/2018/08/guia-evaluacion-impracto-preteccion-datos.pdf

12.4. **Ventanilla virtual de atención especial:** https://www.tudecideseninternet.es/ Canal prioritario. Este canal ha sido habilitado para atender situaciones excepcionalmente delicadas relacionadas con la difusión de fotografías o vídeos de carácter sexual o que muestren actos de agresión, especialmente cuando se pone en grave riesgo los derechos y libertades de personas afectadas que sean españolas o se encuentren en España. Está destinado particularmente para proteger a menores de edad y víctimas de violencia por razón de género. Tanto los afectados como cualquier persona que tenga conocimiento de la difusión de este tipo de contenidos pueden solicitar su retirada inmediata a través de este canal.

12.5. Plan Digital Familiar ayuda a las familias a gestionar el uso de la tecnología en casa, enfocándose en la educación digital de los hijos. Reconoce que padres y educadores a menudo se sienten perdidos debido a la rápida evolución del mundo digital y la información contradictoria. El plan destaca la importancia de que los adultos sean modelos a seguir en el uso responsable de la tecnología y promueve la reflexión sobre el papel de la tecnología en el hogar, con el apoyo de evidencia científica y orientación de pediatras.

La Agencia Española de Protección de Datos (AEPD) está llevando a cabo varias iniciativas para proteger a la infancia y adolescencia en el entorno digital. Una de ellas es el **Plan Digital Familiar**,

Con el apoyo de:
Con el apoyo de:
Cooperación Española

que orienta a las familias sobre el uso responsable de la tecnología, destacando la importancia de que los adultos actúen como modelos y reflexionen sobre el papel de la tecnología en el hogar.

Además, la AEPD ha habilitado una **Ventanilla Virtual de Atención Especial** a través del canal Tu decides en Internet. Este canal está destinado a atender situaciones críticas relacionadas con la difusión de imágenes de contenido sexual o actos de agresión, especialmente cuando dicha difusión pone en ALTO RIESGO los derechos y libertades o la salud física y/o mental de las personas afectadas. Si no se ha logrado la retirada de estas imágenes a través de los canales del prestador de servicios, puede presentar una reclamación en esta vía. Deberá describir detalladamente las circunstancias de la difusión no consentida, indicando si la persona afectada es víctima de violencia de género, abuso, agresión sexual, acoso, o pertenece a colectivos especialmente vulnerables como menores de edad (especificando si es menor de catorce años), personas con discapacidad, enfermedad grave o en riesgo de exclusión social.

En términos de **potestades de investigación y sanción**, la AEPD prioriza la verificación de edad en páginas web de contenido para adultos, como la pornografía. Ha sancionado varias páginas web, analizado el funcionamiento de terceros de confianza para la verificación de edad, y colabora con autoridades internacionales cuando las empresas están fuera de España. También está realizando un análisis de algoritmos y patrones adictivos que afectan el comportamiento y decisiones de los usuarios, especialmente en relación con menores.

La AEPD también ha lanzado el **Pacto Digital para la Protección de las Personas**, una iniciativa que promueve un compromiso con la privacidad en las políticas de sostenibilidad y modelos de negocio. Este pacto busca equilibrar el derecho a la protección de datos con la innovación, la ética y la competitividad empresarial. Está abierto a organizaciones jurídicas que deseen asumir los compromisos reflejados en la carta de adhesión. Más información está disponible en este enlace.

Finalmente, la **"Carta de Adhesión: Por un Pacto Digital para la Protección de las Personas"** busca fortalecer las relaciones con medios de comunicación y organizaciones para informar sobre la protección de la privacidad y concienciar sobre el canal prioritario para la retirada de contenidos sexuales o violentos difundidos sin consentimiento. Más detalles están disponibles en este enlace.

13. Guatemala:

13.1. Hacia una ley de protección de datos. Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0): https://creativecommons.org/licenses/by-sa/4.0/ "La situación actual hace de

urgente importancia la formulación de políticas públicas que protejan a la ciudadanía, con un enfoque de derechos humanos, en el mundo físico y digital. Hoy, la comunidad internacional ve con gran importancia el reconocimiento de derechos de privacidad en línea, particularmente en la protección de datos personales. En nuestra sociedad actual, los ciudadanos comparten sus datos personales cuando participan en discusiones, realizan transacciones, o en actividades tan cotidianas como compras de víveres a través de las plataformas. Lo que es más importante, todos los datos no han sido creados igualmente. Poblaciones marginalizadas y voces de disidencia política son especialmente vulnerables a vigilancia policial. La historia de Guatemala de alta pobreza, feminicidio y violencia sistemática hace de este país necesidades únicas en materia de protección de datos. Este informe analiza brevemente la regulación de la protección de datos en Guatemala, pasando por una discusión más amplia de los principios y prácticas regionales e internacionales de regulación de la protección de datos, a través de la lente de las normas internacionales de protección de informes, tal como se resume en el Reglamento General de Protección de Datos de Europa. Por último, tras un estudio de la legislación nacional propuesta y aplicada, la lista exhaustiva de buenas prácticas y recomendaciones a medida que Guatemala continúa conformando y mejorando su política de intercambio de datos y la protección de los derechos de privacidad de los usuarios." https://www.ipandetec.org/wp-content/uploads/2021/06/GUATEMALA.pdf

13.2. Estudio sobre protección de datos en el sector de salud: https://www.acnur.org/es-es/media/informe-del-sistema-de-proteccion-en-guatemala-segunda-edicion

14. Honduras: No se encontró información pública al respecto.

15. México

15.1. Suprema Corte de Justicia de la Nación. *Guía de Protección de Datos Personales*. 2019. https://www.scjn.gob.mx/sites/default/files/pagina_transparencia/documento/2019-07/Guia_Proteccion_Datos_Personales_V2.pdf.

15.2. **Guía para la Protección de Datos Personales con Perspectiva de Gestión Documental y Archivos.** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2014.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

https://home.inai.org.mx/wp-content/uploads/GuiaPDPGestionDocumental.pdf.
Con la reforma constitucional en materia de transparencia del año 2014, se dotó al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de autonomía constitucional y le otorgó la encomienda de encabezar el Sistema Nacional de Transparencia. Esto tiene el objetivo de establecer el piso mínimo de bases y principios sobre los cuales descansan los derechos de acceso a la información y a la protección de datos personales. En este sentido, el último párrafo del artículo 6, apartado A, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos impone el deber al organismo garante de colaborar con la Auditoría Superior de la Federación, la entidad especializada en archivos, el organismo encargado de la información estadística y geográfica, y los organismos garantes de las entidades federativas para fortalecer la rendición de cuentas del Estado Mexicano.

16. **Nicaragua:** No se encontró información pública al respecto.

17. **Panamá**

17.1. Guia para cumplir la normativa sobre proteccion de datos personales: “Protegiendo los datos personales, protegemos a los ciudadanos en el sector público” https://www.antai.gob.pa/wp-content/uploads/2024/01/Guia-para-cumplir-la-normativa-1.pdf

17.2. **Guías:** Guías de Protección de Datos Personales https://youtu.be/tYWdNK89d3g?si=3fZqEmDPdXXrD_sa

18. **Paraguay:**

18.1. **Guía:** La presente guía está orientada a proporcionar criterios técnicos para la publicación de datos o información en formato de datos abiertos. https://www.datos.gov.py/vista-guias

18.2. Campaña "El retorno de los Pyrawebs" (2017): "El retorno de los Pyrawebs" es una serie ilustrada co-creada con El Surtidor que aborda la falta de protección de datos personales en Paraguay. A través de cinco capítulos, la serie explora cómo han evolucionado los mecanismos de vigilancia, los riesgos diarios asociados con la provisión de datos personales y las violaciones de derechos que ocurren debido al uso arbitrario de esta información. La campaña destaca el estado de indefensión en

Con el apoyo de:
Con el apoyo de:
Cooperación Española

el que se encuentran los ciudadanos paraguayos debido a la falta de estándares mínimos de protección de datos personales en el país. **(https://www.datospersonales.org.py/el-retorno-de-los-pyrawebs/)**

19. Perú:

19.1. Guía: Manual de protección de datos personales" https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf "Cuando contratamos servicios de agua o luz, damos nuestro documento de identidad y señalamos nuestro domicilio; cuando adquirimos productos mediante el uso de tarjetas de crédito, firmamos para autorizar la transacción; cuando solicitamos un producto por delivery, brindamos el celular y la dirección de destino; incluso, cuando nos registramos en alguna red social o descargamos una app entregamos datos de identificación. De allí y ante la preocupación que existe sobre el tratamiento de nuestra información personal, la Adjuntía en Asuntos Constitucionales de la Defensoría del Pueblo ha desarrollado este "Manual de protección de datos personales" con el objetivo de que la ciudadanía pueda conocer en forma clara, sencilla y didáctica qué son estos datos, cuál es el tratamiento que se les puede dar, cuáles son sus derechos frente a los bancos de datos, qué instrumentos tiene para defenderlos, así como la entidad encargada de protegerlos. La recopilación y tratamiento permanente de esta información por parte de entidades públicas y privadas, requiere de mecanismos que permitan protegerlos adecuadamente y garanticen la posibilidad de efectuar un control sobre ellos, con la finalidad de evitar que un tratamiento indebido afecte directamente la intimidad personal y/o familiar, o sea utilizado para cometer actos ilícitos."

19.2. **Guía para oficial de protección de datos (2023):** El presente documento busca informar, de manera práctica y sencilla, los alcances del rol que debe cumplir el Oficial de Datos Personales dentro de sus respectivas entidades públicas, así como brindar pautas y recomendaciones para el cumplimiento de los principios, obligaciones y derechos contemplados en la Ley N.° 29733, Ley de Protección de Datos Personales y su Reglamento, aprobado por Decreto Supremo Nro. 003-2013-JUS. (https://www.gob.pe/institucion/anpd/informes-publicaciones/4217939-instructivo-para-oficiales-de-datos-personales)

Con el apoyo de:
Con el apoyo de:
Cooperación Española

19.3. La Autoridad Nacional de Protección de Datos Personales (ANPD) del Ministerio de Justicia y Derechos Humanos (MINJUSDH) aprobó la "Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales", que garantiza el resguardo de la información, las medidas de seguridad, confidencialidad, entre otros, en cumplimiento de los estándares internacionales. Permitirá un mayor dinamismo en la transferencia de datos, favoreciendo el flujo económico, el comercio exterior, el comercio electrónico, entre otros. La ANPD considera que la Guía constituye un documento de orientación particularmente relevante para superar las limitaciones en las transferencias internacionales de datos, que contribuirá a que estas se realicen bajo condiciones que resguarden el derecho de los titulares de los datos, en armonía con la Ley N.º 29733, Ley de Protección de Datos Personales y su Reglamento. El documento se basa en la Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales publicada por la Secretaría Permanente de la Red Iberoamericana de Protección de Datos (RIPD). La ANPD estima que la Guía de la RIPD debe ser considerada para su aplicación en nuestro país con el fin de que las transferencias internacionales de datos se realicen bajo condiciones que resguarden el derecho de los titulares de los mismos. La Guía, junto con la Resolución Directoral N.º 74-2022-JUS/DGTAIPD que la aprueba para su aplicación en Perú: https://www.gob.pe/institucion/minjus/normas-legales/3617286-0074-2022-jus-dgtaipd

19.4. **Video educativo:** ¿En qué consiste el derecho a la protección de datos personales? https://youtu.be/-zn6vEbRl0s?si=w8LsjTqneOwSbIOA

19.5. **Trámites virtuales:**

- Consultar el Registro Nacional de Protección de Datos Personales.
- Inscribir el banco de datos en el Registro Nacional de Protección de Datos Personales.
- Modificar banco de datos en el Registro Nacional de Protección de Datos Personales.
- Denunciar el mal uso de datos personales

Finalmente, la autoridad peruana creó un emoji representativo para **campañas educativas:** "Datito" es un personaje creado por la Autoridad Nacional de Protección de Datos Personales (ANPD) del Ministerio de Justicia y Derechos Humanos (MINJUSDH) para educar al público sobre la protección

Con el apoyo de:
Con el apoyo de:
Cooperación Española

de datos personales. A través de diferentes situaciones, "Datito" alerta sobre los peligros de aceptar contactos desconocidos en redes sociales y usar contraseñas fáciles de recordar. También proporciona recomendaciones sobre cómo manejar datos al comprar, cómo reaccionar ante correos sospechosos y qué hacer al llenar formularios. La ANPD ha creado una serie de videos en TikTok que abordan temas como: Protección de datos personales; No entregar el DNI físico; Compras por Internet

20. Portugal: No se encontró información pública al respecto.

21. Uruguay:

21.1. Guía general de protección de datos personales en Uruguay. Enero de 2022. El documento orienta sobre el Derecho a la Protección de Datos Personales y los medios para facilitar su ejercicio, y espera constituirse en una herramienta de capacitación útil para todas las personas.En: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay

21.2. *Guía Criterios de Disociación de Datos Personales*. Versión 2.0 – Año 2017. Resolución Nº 68/017, April 26, 2017. La Unidad Reguladora y de Control de Datos Personales aprobó, mediante la Resolución Nº 68/017 del 26 de abril de 2017, el documento *Criterios de Disociación de Datos Personales* conforme al Decreto N° 54/017, del 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, del 19 de diciembre de 2015. Este documento establece que las Entidades Públicas, obligadas por la Ley N° 18.381, del 17 de octubre de 2008, deben publicar la información contenida en los artículos 5° de la Ley y 38 y 40 del Decreto N° 232/010, del 2 de agosto de 2010, en formato de dato abierto. Este e-book presenta diversos criterios para evitar la identificación de datos personales en la información que debe publicarse como dato abierto, incluyendo técnicas como seudonimización, disociación y anonimización. Su objetivo es que las personas que utilicen estas técnicas sigan los lineamientos proporcionados en el e-book para minimizar la posibilidad de reidentificación del titular del dato, considerando que esta es una

actividad dinámica que evoluciona con la aparición de nuevos mecanismos de reidentificación. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales/guia-criterios-disociacion

21.3. *Guía de Usuario para la Inscripción de Bases de Datos en el Sistema de Gestión de la URCDP*. January 15, 2018. La *Guía de Usuario para la Inscripción de Bases de Datos en el Sistema de Gestión de la URCDP*, publicada el 15 de enero de 2018, proporciona orientaciones para el uso del sistema de gestión de la URCDP. Este sistema permite a todos los responsables de bases de datos (entidades públicas, personas físicas o jurídicas) realizar gestiones relacionadas con el registro de bases de datos de manera fácil y sencilla a través de la web, en cualquier momento y lugar, sin necesidad de desplazarse. Además, el sistema permite inscribir Códigos de Conducta relativos a la Protección de Datos Personales y comunicar la designación de Delegados de Protección de Datos Personales, conforme al artículo 40 de la Ley N° 19.670, del 15 de octubre de 2018.https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-usuario-para-inscripcion-bases-datos-sistema-gestion-urcdp

21.4. *Delegado de Protección de Datos Personales: Documento de Trabajo*. September 26, 2019. El *Documento de Trabajo sobre el Delegado de Protección de Datos Personales*, publicado el 26 de septiembre de 2019, aborda las modificaciones introducidas a la Ley de Protección de Datos Personales, cuyo objetivo es establecer un marco moderno basado en la Rendición de Cuentas. En este contexto, el delegado de Protección de Datos Personales juega un papel crucial, siendo considerado un elemento esencial para promover la protección de los datos personales. El documento subraya que el delegado tiene funciones de gran importancia dentro de un modelo de responsabilidad proactiva.

22. **Venezuela:** No se encontró información pública al respecto.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Anexo 7. Algunas políticas públicas sobre tratamiento de datos personales en los países miembros de la SEGIB

A la fecha se han identificado los siguientes documentos que directa e indirectamente contienen información sobre algunas políticas públicas sobre tratamiento de datos personales:

Argentina:

- Política de Protección de Datos Personales de diciembre 2021. Registro Nacional de las personas. La Política de Protección de Datos Personales de la Dirección Nacional del Registro Nacional de las Personas (en adelante, la "Política") tiene como objetivo resguardar y proteger el derecho a la privacidad de las personas físicas cuyos Datos Personales sean objeto de tratamiento por parte del Organismo.https://servicios.infoleg.gob.ar/infolegInternet/anexos/355000-359999/359224/disp1.pdf
- Programa Nacional "Con Vos en la Web" en Argentina, que se ejecuta por intermedio de la Agencia de Acceso a la Información Pública (AAIP). Dicho programa es una iniciativa del Ministerio de Justicia, dirigido a concienciar y desarrollar, en padres, docentes, alumnos y ciudadanía en general: "conductas seguras y responsables en el uso de dispositivos tecnológicos conectados a Internet y en el manejo de sus datos privados y personales"

Bolivia:

- A pesar de no existir una normativa específica de protección de datos personales en Bolivia, se crearon varias políticas públicas y proyectos con posibilidad de afectar potencialmente la privacidad de toda la ciudadanía.
- Ley de ciudadanía digital:La ciudadanía digital se encuentra plasmada, como se mencionó, en la Ley 1080 que fue promulgada en julio de 2018. De acuerdo a esta, para ejercer la ciudadanía digital, es necesario realizar un proceso de registro y autenticación para recibir una credencial que sólo puede ser usada por el interesado/a (Art. 5). Este registro consiste en: darse de alta en el sistema con una huella digital y fotografía, firma digital y confirmación vía correo electrónico y SMS. Desde ese aspecto, la Ley de ciudadanía digital sigue una tendencia vista en varios otros países que es la de proveer una sola identidad compatible e

Con el apoyo de:
Con el apoyo de:
Cooperación Española

indivisible entre la identidad natural de un/a ciudadano/a de un Estado y aquella de tipo digital. Es decir, se hace una compatibilización y/o asociación de datos entre la persona natural y los registros online a través del uso de datos personales.

- PLAN NACIONAL DE SEGURIDAD CIUDADANA-BOL 110: en implementación de su primera fase. Desde el año 2012 se empezó a implementar el nuevo Plan Nacional de Seguridad Ciudadana en Bolivia. Este se encuentra normado a través de la Ley 264. Esta normativa, dedica el Capítulo IV, a medidas de prevención tecnológica, las cuales incluyen "sistemas de monitoreo y vigilancia electrónica para el control y prevención de delitos, faltas y contravenciones" (Art. 47), cámaras de seguridad en "empresas prestadoras de servicios públicos, entidades financieras bancarias, las entidades públicas y centros de esparcimiento público y privado con acceso masivo de personas" (Art. 50). La Policía Boliviana tendrá acceso a las grabaciones y sistemas con fines investigativos. A su vez, el Ministerio de Gobierno y la Policía Boliviana suscribirán convenios con empresas y cooperativas telefónicas para el uso de su infraestructura de red para el funcionamiento de los sistemas de seguridad (Art. 51).https://library.fes.de/pdf-files/bueros/bolivien/16242.pdf

Ecuador:

- "Mis datos soy yo", desarrollada, a partir de 2018, por la Dirección Nacional de Registros Públicos (Dinarp), que tiene por objetivo enseñar a los jóvenes la importancia de la protección de su información personal. Sin embargo, en septiembre de 2020, el Consejo Nacional para la Igualdad Intergeneracional (CNII) implementó la "Política pública por una internet segura para niños, niñas y adolescentes", la cual se orienta a "promover una cultura preventiva para el uso seguro de la internet y las tecnologías digitales, así como el adecuado seguimiento y sanción en caso de vulneraciones de derechos" (CNII, 2020, p. 6). Si bien son iniciativas dirigidas a menores de edad, el vacío existente frente a la emergencia sanitaria ha dejado al descubierto la carencia de políticas públicas en la materia. https://www.redalyc.org/journal/6842/684272393004/html/

Uruguay:

- "Tus Datos Valen. Cuídalos" es una propuesta educativa que introduce la temática de protección de datos personales a través de una mirada integral en la que confluyen niños, padres y docentes. Se trata de una iniciativa liderada por la Unidad Reguladora y de Control

de Datos Personales (URCDP) en Uruguay y apoyada por socios estratégicos tales como la Administración Nacional de Educación Pública - Consejo de Educación Inicial y Primaria (ANEP – CEIP), órgano rector de la educación en Uruguay; y Plan Ceibal, que se encarga de gestionar en nuestro país el programa para la Conectividad Educativa de Informática Básica para el Aprendizaje en Línea, tendiente a promover la inclusión digital para un mayor y mejor acceso a la educación y a la cultura. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/campanas/tus-datos-valen

Anexo 8. Elementos iniciales para establecer la la eficacia y operabilidad de los marcos normativos de los países iberoamericanos y potencial coordinación entre ellos.

A continuación, nos referiremos a los siguientes aspectos requeridos por la SIGEB:

Eficacia y operabilidad de los marcos normativos de los países Iberoamericanos

Actualmente no existe un mecanismo de medición ni indicadores de la eficacia y operabilidad de los marcos normativos sobre protección de datos en los países miembros de la SEGIB.

Las autoridades de protección de datos han realizado diferentes actividades para cumplir sus funciones dentro del marco de sus competencias legales. No obstante, los resultados obtenidos varían considerablemente entre ellas

En lo referente a los países europeos, la Comisión Europea (CE) publicó el 25 de julio de 20245 el segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Dentro de

Con el apoyo de:
Con el apoyo de:
Cooperación Española

los aspectos mas relevantes destacamos lo siguientes por ser conexos con los temas y objetivos de este estudio:

- **Multas por infracción de la regulación de datos**

Señala la CE que "en los últimos años, las autoridades de protección de datos han experimentado un importante repunte en las actividades de control del cumplimiento, especialmente la imposición de multas sustanciales en casos históricos contra grandes multinacionales tecnológicas.(..). Esto ha llevado a las empresas privadas a «tomarse en serio la protección de datos» y ha contribuido a integrar una cultura del cumplimiento en las organizaciones"[191].

En adición a la multas por infracciones a la regulación sobre datos personales, las medidas correctivas mas utilizadas fueron "las advertencias, los apercibimiento y las órdenes de cumplimiento del RGDP".

Se destacan estos resultados[192]:

- "Las autoridades ha iniciado mas de 20,000 investigaciones por iniciativa propia
- "Las autoridades reciben mas de 100,000 reclamaciones al año. "En 2022, (..) el mayor número de reclamaciones se registró en Alemania (32300), Italia (30880), España (15 128),

[191] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 5
[192] Cfr. Estos son resultados son tomado del siguiente informe: CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Pág. 6

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Países Bajos (13133) y Francia (12193), mientras que el número más bajo lo registraron Liechtenstein (40), Islandia (140) y Croacia (271)." [193]

- "Más de 20 000 reclamaciones se han resuelto por medio de arreglos amistosos, y Austria, Hungría, Luxemburgo e Irlanda son los países donde se utilizan con más frecuencia.

- "En 2022, el país con el mayor número de decisiones por las que se impusieron medidas correctoras fue Alemania (3 261), seguido de España (774), Lituania (308) y Estonia (332). El menor número de medidas correctoras se impuso en Liechtenstein (8), Chequia (8), Islandia (10), Países Bajos (17) y Luxemburgo (22).

- "Las autoridades de protección de datos han impuesto más de 6680 multas por un importe aproximado de 4 200 millones EUR. El mayor importe total de las multas fue impuesto por la autoridad de Irlanda (2800 millones EUR), seguido de Luxemburgo (746 millones EUR), Italia (197 millones EUR) y Francia (131 millones EUR). Por su parte, los importes más bajos corresponden a Liechtenstein (9 600 EUR), Estonia (201 000 EUR) y Lituania (435 000 EUR). "

- "Todas las autoridades impusieron multas administrativas, excepto Dinamarca, que no prevé dicha posibilidad. El mayor número de multas se impuso en Alemania (2106) y España (1596), y el menor, en Liechtenstein (3), Islandia (15) y Finlandia (20). "

-

En adición a lo establecido en dicho informe, en algunas páginas web de las autoridades de protección de datos se encuentra cierta información sobre los resultados de su labor en los informes de gestión. De allí se puede extraer algo sobre los resultados obtenidos que, en

[193] Cfr. CE, 2024. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos. Bruselas, 25.7.2024 COM(2024) 357 final. Nota de pie de página No. 30 de la página 6.

últimas, se relacionan, parcialmente, con la eficacia y operabilidad. No obstante, se debe tener presente lo siguiente:

1. No todas las autoridades presentan informes de gestión anual.
2. En los casos que existen estos informes, los ítems o contenidos no son comparables porque no son iguales

No existe una sola forma de medir la eficacia de las normas de protección de datos. Esta puede medirse, entre otras y a título de ejemplo, a través de la aplicación de sanciones y multas. Este enfoque nos permite evaluar no solo la existencia de leyes, sino también su implementación práctica y el compromiso de las autoridades para hacerlas cumplir. Las sanciones y multas actúan como disuasores para potenciales infractores y reflejan la seriedad con la que un país aborda la protección de datos de sus ciudadanos. En el panorama analizado, se observa una clara disparidad entre países en cuanto a la aplicación de estas medidas. Algunas naciones destacan por su enfoque proactivo y riguroso, mientras que otras muestran una aplicación limitada o inexistente, lo que podría indicar deficiencias en sus marcos regulatorios o en su capacidad de ejecución.

Entre los países con una aplicación más robusta se encuentra España, donde la Agencia Española de Protección de Datos (AEPD) impuso 357 sanciones en 2023, sumando más de 16 millones de euros (Cinco Días, 2024). Este nivel de actividad sancionadora sugiere un sistema de protección de datos maduro y activo.

Portugal también demuestra un compromiso significativo, con multas notables como la de 4.3 millones de euros impuesta al Instituto Nacional de Estadística en 2021 (The Portugal News, 2022). Estas acciones indican una aplicación estricta del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

En América Latina, países como Colombia, Brasil, México y Perú están emergiendo como líderes regionales en la aplicación de normas de protección de datos. Colombia ha sido líder en inic iar y culminar investigaciones de impacto masivo que afectan a millones de personas contra Facebook, Uber, TikTok, WhatsApp, Google y Zoom. Esa línea ha sido seguida por Brasil, que ha tomado medidas contra gigantes tecnológicos como Meta, imponiendo multas diarias de 50.000 reales por incumplimientos (La República, s .f.). México, a través del INAI, recaudó más de 46 millones de pesos

Con el apoyo de:
Con el apoyo de:
Cooperación Española

en multas en 2023 (Forbes México, s.f.), mientras que Perú impuso sanciones por más de 7.6 millones de soles en el mismo año (Gobierno del Perú, 2024).

Argentina muestra un enfoque estructurado, con la AAIP imponiendo multas entre 40.001 y 80.001 pesos argentinos por infracciones específicas (Ojam Bullrich Flanzbaum, s.f.). Aunque las cantidades son menores en comparación con otros países, indican un sistema de sanciones en funcionamiento.

Otros países como Andorra y Costa Rica han establecido sistemas de sanciones, pero con una actividad más moderada. Andorra gestiona entre 15 y 20 expedientes sancionadores anualmente (L'Agència de Protecció de Dades gestiona una vintena d'expedients sancionadors cada any, 2014), mientras que Costa Rica ha establecido multas que van desde ¢2,2 millones hasta ¢13,5 millones (La República, s.f.).

En contraste, países como Cuba, República Dominicana, Guatemala, Honduras, Nicaragua, Paraguay y Venezuela no proporcionaron información específica sobre sanciones o multas. Esta falta de datos podría indicar una aplicación limitada de las normas de protección de datos o la ausencia de un marco regulatorio robusto.

La eficiencia de las normas de protección de datos se refleja en la capacidad de un país para detectar infracciones, aplicar sanciones y disuadir futuras violaciones. Los países que muestran una actividad sancionadora más intensa generalmente indican un sistema más eficaz, ya que demuestran: i) una infraestructura legal y administrativa capaz de identificar y procesar infracciones; ii) un compromiso activo con la protección de los derechos de los ciudadanos en materia de datos personales; y, iii) un efecto disuasorio sobre potenciales infractores, promoviendo un mejor cumplimiento general.

Sin embargo, es importante notar que la mera presencia de sanciones no garantiza la eficacia total del sistema. Algunos factores como la proporcionalidad de las multas, la consistencia en su aplicación y la capacidad de las autoridades para hacer cumplir las sanciones también juegan un papel crucial.

En las siguientes líneas destacamos alguna información relevante sobre los países miembros de la SEGIB cuya información es pública:

1. **Andorra**

Con el apoyo de:
Con el apoyo de:
Cooperación Española

1.1. Sanciones: La Agencia de Protección de Datos de Andorra (APDA) gestiona entre 15 y 20 expedientes sancionadores cada año de casos de vulneración de la protección de los datos personales. Según ha indicado el director de la APDA, Joan Crespo, es una proporción 'bastante similar' a la de los países vecinos, aunque la 'relación de proximidad' que existe en el Principado por sus dimensiones hace que los usuarios sean más bien reacios a denunciar. La Agencia celebró este martes el Día europeo de la protección de datos con una jornada de puertas abiertas y la edición de un folleto informativo. La recomendación general, según Crespo, es que 'cuanta menos información de carácter personal se cuelgue en las redes, mejor'. L'Agència de Protecció de Dades gestiona una vintena d'expedients sancionadors cada any (2014) https://youtu.be/oNzOM_m_sg8?si=9c0SN0vQ94veCOGF

1.2. Se abren 80 expedientes sancionadores en lo que va de año. (2023) https://www.bondia.ad/societat/els-banders-obren-80-expedients-sancionadors-des-de-principi-dany

2. Argentina

2.1. **Sanciones:** Durante los primeros meses de 2022, la Agencia de Acceso a la Información Pública (AAIP) impuso sanciones a varias organizaciones por infracciones a la Ley de Protección de Datos Personales N° 25.326. Entre los casos destacaron una distribuidora de energía, una institución médica, una entidad crediticia y un fideicomiso financiero, todas sancionadas principalmente por no tener sus bases de datos inscriptas en el Registro Nacional y por no responder adecuadamente a las solicitudes de los denunciantes, con multas que oscilaron entre 40.001 y 80.001 pesos argentinos. https://www.ojambf.com/nuevas-sanciones-impuestas-por-la-autoridad-de-proteccion-de-datos/

2.2. Informe de gestión: (2023) El Informe de Gestión 2023 de la Agencia de Acceso a la Información Pública (AAIP) detalla las acciones realizadas para monitorear la transparencia en la gestión pública, garantizar el acceso a la información y proteger datos personales. Entre los hitos destacados se incluyen el fortalecimiento del seguimiento de políticas de transparencia, la actualización de la Ley de Protección de Datos Personales, la consolidación del Consejo Federal para la Transparencia, y la organización del XXIV encuentro de la Red de Transparencia y Acceso a la Información de Iberoamérica. https://www.argentina.gob.ar/noticias/la-aaip-presenta-su-informe-de-gestion-2023 Durante 2023, se presentaron 11.615

Con el apoyo de:
Con el apoyo de:
Cooperación Española

solicitudes de información ante los sujetos obligados de la Ley N° 27.275, un aumento del 29,90% respecto al año anterior. La AAIP recibió 27 solicitudes, relacionadas principalmente con consultas sobre la Ley de Acceso a la Información, denuncias y resoluciones sancionatorias bajo la Ley de Protección de Datos Personales, el Registro Nacional "No Llame", y cuestiones administrativas y de recursos humanos.

3. **Bolivia**:

3.1. Informe de gestión (2022) Durante el año 2022 se gestionaron 769 casos de incidentes y vulnerabilidades informáticas, que corresponden a reportes nuevos y abiertos en períodos anteriores. Del total de casos, 563 fueron resueltos a través de una correcta comunicación, seguimiento y validación con las entidades afectadas y 206 se encuentran abiertos, los cuales están siendo gestionados para su solución; los resultados serán reflejados en siguientes informes. En la gestión 2022 se registraron 107 nuevos incidentes informáticos, que fueron categorizados de acuerdo al detalle, representado por la siguiente tabla y su respectivo gráfico y 20,6% hacen partner de crímenes contra la obtención de información https://www.cgii.gob.bo/sites/default/files/IGIV-Gestion_2022-firmado.pdf

4. Brasil:

4.1. **Multa:** La Autoridad Nacional de Protección de Datos de Brasil (ANPD) ha suspendido con efecto inmediato la nueva política de privacidad de Meta relacionada con el uso de datos personales para entrenar sistemas de inteligencia artificial generativa. Meta deberá modificar su política de privacidad para excluir dicha sección, y enfrenta una multa diaria de 50.000 reales (US$8.836,58) si no cumple con la medida, la cual afecta a todos sus productos, incluidos los de personas que no son usuarios de sus plataformas. https://www.larepublica.co/globoeconomia/autoridad-nacional-de-proteccion-de-datos-de-brasil-suspende-una-politica-de-meta-3899143

4.2. **Suspensión:** La agencia de protección de datos de Brasil, la ANPD, ha ordenado a Meta que detenga su entrenamiento de sistemas de IA generativa en el país. La ANPD citó preocupaciones sobre la privacidad de los usuarios y el potencial de daño, y según la última declaración de Meta a TechCrunch, la compañía está pisando el freno en Brasil por ahora, mientras lo soluciona todo.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

(https://www.notebookcheck.org/Brasil-paraliza-el-entrenamiento-de-IA-generativa-de-Meta-por-temor-a-la-privacidad-de-los-datos.864890.0.html)

5. Colombia:

De conformidad con el informe de gestión del año 2023 de la Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio (SIC), los resultados más sobresalientes en dicho año fueron son los siguientes:

En el ejercicio de las **funciones sancionatoria**, se destacan los siguientes indicadores:

- Sanciones**.** Se impusieron 93 sanciones por un valor de $ 4.934.169.668.
- Ordenes administrativas. Se impartieron 2.508 órdenes administrativas.
- Se impuso la sanción más alta, desde la creación de esta dependencia, a Comunicación Celular Comcel (Claro) por el indebido Tratamiento de datos personales sin autorización de los titulares mediante el programa "Amigos que te premian", por un monto de $1.306.000.000 millones de pesos.
- Se ejerció por primera vez la facultad sancionatoria consistente en el cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles, así como, se suspendieron las actividades de algunas sociedades.

En el ejercicio de las **funciones de carácter preventivo**, se destacan los siguientes logros:

- Se elaboró un nuevo Estudio de Medidas de Seguridad en el Tratamiento de Datos el que por primera vez tiene un enfoque regional. Aquel es la base para impartir las ordenes administrativas de carácter preventivo a los sujetos obligados. Con este documento, se pueden tomar decisiones atendiendo las necesidades particulares de cada región.

- Se logró que en el marco de las ordenes administrativas impartidas a Grupo Meta (WhatsApp, Facebook, Instagram, Threads etc), aquella implementara dos correos específicos y exclusivos para la Superintendencia de Industria y Comercio para la atención eficiente, efectiva y eficaz de las quejas de los usuarios de sus redes, así como para la notificación de actos administrativos que sean del caso, propiciando una comunicación más fluida que no se daba con anterioridad a la implementación de tales correos.

- Se realizaron campañas de divulgación dirigidas a titulares y sujetos obligados en temas relacionados con suplantación de identidad y buenas prácticas empresariales en el tratamiento de Datos Personales (2023).

Se evidencia que cada año aumenta el número de quejas ciudadanas por presuntas infracciones a la regulación sobre protección de datos.

6. **Costa Rica:**

6.1. Sanciones: En 2020, el presidente Carlos Alvarado admitió errores en el uso de datos personales por parte de una unidad de análisis de datos del gobierno y anunció su detención para permitir una investigación completa. Según la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, las sanciones por el uso indebido de datos van desde ¢2,2 millones hasta ¢13,5 millones, dependiendo de la gravedad de la infracción. La situación ha llevado a una comisión especial en el Congreso para investigar el asunto. (https://www.larepublica.net/noticia/mal-uso-de-datos-privados-se-castiga-con-multa-de-hasta-135-millones)

7. **Cuba**: No se encontró información pública al respecto.

8. **Chile:**

8.1. **Sanciones:** A solicitud de la Comisión de Constitución, Legislación, Justicia y Reglamento de la Cámara de Diputadas y Diputados, en el marco del estudio del proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletines 11.144-07 y 11.092-07), el presente informe, en primer lugar, se refiere al concepto de sanción administrativa y la aplicación del principio de proporcionalidad a las mismas. Con este objeto se analiza tanto en la doctrina nacional y en sentencias del Tribunal Constitucional respecto de esta materia. En segundo lugar, se revisan los regímenes sancionatorios que la ley les reconoce a diversos órganos de control, principalmente

Con el apoyo de:
Con el apoyo de:
Cooperación Española

de tipo sectoriales. Al efecto se da cuenta de las normas que configuran su potestad sancionatoria, especialmente las facultades para imponer multas a las entidades fiscalizadas. A este respecto se detallan las infracciones asociadas a las respectivas multas, el monto o entidad de las multas que cada órgano puede imponer, las reglas en relación con reincidencias u otros factores que incrementan su monto, y los criterios dispuestos por cada estatuto para fijar el monto dentro del rango establecido en la ley. Finalmente, se revisa la situación en el derecho comparado en relación con las sanciones aplicables por infracción a las leyes sobre protección de datos personales. Con este objeto se seleccionaron siete países tanto de Latinoamérica como de Europa y, además la regulación en la materia de la Unión Europea, pues ella dispone de un Reglamento que regula la materia entre sus países miembros. Biblioteca del Congreso Nacional de Chile. *Sanciones Administrativas en Materia de Protección de Datos Personales*. Santiago de Chile: BCN, 2022. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33803/1/BCN_Sanciones_Administrativas__2022.pdf.

8.2. **Multas:** Multas y Protección de Datos." *DF Lab*, Diario Financiero, 2022. https://www.df.cl/df-lab/transformacion-digital/df-lab-opinion-multas-y-proteccion-de-datos. La economía digital ha transformado los negocios, generando nuevos riesgos para las empresas, especialmente en términos de daño reputacional y sanciones económicas por incumplimiento de normativas. Un ejemplo notable es la reciente multa de 1.200 millones de euros impuesta a Meta por el regulador irlandés por violar el GDPR en las transferencias de datos de usuarios europeos a Estados Unidos. El GDPR ofrece a las autoridades europeas diversas herramientas sancionadoras para infracciones de protección de datos. Estas incluyen multas de hasta 20 millones de euros o el 4% del volumen de negocio anual mundial, además de apercibimientos o prohibiciones de tratamiento de datos. Las autoridades deben asegurar que las sanciones sean efectivas, proporcionadas y disuasorias. Chile está considerando implementar una ley similar al GDPR europeo. Esto plantea la pregunta de qué consecuencias podrían enfrentar las empresas en Chile en casos de "presunta negligencia grave" similares al de Meta en Europa, una vez que se establezca esta nueva normativa de protección de datos.

9. **R. Dominicana:** No se encontró información pública al respecto.

10. **Ecuador:** No se encontró información pública al respecto.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

11. El Salvador

11.1. **Multas:** Henríquez, Gerardo. "Las multas impuestas obedecen a un 87% en el caso de prácticas anticompetitivas y 13% en el caso de otras infracciones." Superintendencia de Competencia, 2018. https://www.sc.gob.sv/index.php/las-multas-impuestas-por-la-sc-y-su-ejecucion/. Las entidades públicas en Ecuador han sufrido varias brechas de seguridad de datos personales. En septiembre de 2019, ocurrió la mayor filtración de la historia del país, exponiendo datos personales de millones de ciudadanos en un servidor en Miami, manejado por Novaestrat. En 2021, hubo nuevas vulneraciones en el Ministerio de Salud y la Corporación Nacional de Telecomunicaciones (CNT), afectando los servicios de atención al cliente. Con la Ley de Protección de Datos, las empresas públicas tienen mayor responsabilidad en la seguridad de los datos y pueden ser sancionadas por violaciones. La CNT afirma haber reforzado sus controles, aunque no cuenta con un delegado de protección de datos, figura obligatoria según la ley. Banecuador, en cambio, ya tiene un delegado de protección de datos y solicita el consentimiento de sus clientes para varios servicios.

12. España:

12.1. **Multas:** La Agencia Española de Protección de Datos (AEPD) ha impuesto 357 sanciones en 2023 por un importe total que asciende a más de 16 millones de euros, según la información recogida por LA LEY a partir de lo publicado por la AEPD hasta el 24 de enero de 2024. Unas cifras que se espera que aumenten ligeramente cuando la agencia termine de publicar todas sus resoluciones del pasado año y lance su memoria anual de 2023, prevista para la próxima primavera. (https://cincodias.elpais.com/cincodias/2024/01/26/legal/1706263168_397932.html)

12.2. **Multas**: La Agencia Española de Protección de Datos ha impuesto una multa de 550.000 euros a Glovo por un tratamiento abusivo de los datos personales de los repartidores que utilizan la plataforma. El regulador considera que la compañía lleva a cabo una vigilancia excesiva de los riders y además no impide que cualquier persona de la empresa con acceso a su sistema interno de repartos pueda consultar un enorme número de datos sobre ellos, incluso aunque el repartidor se encuentren en un país diferente. https://www.aepd.es/documento/ps-00209-2022.pdf

Con el apoyo de:
Con el apoyo de:
Cooperación Española

13. **Guatemala:** No se encontró información pública al respecto.

14. **Honduras:** No se encontró información pública al respecto.

15. **México:**

15.1. **Multas** por infracciones a Ley de Protección de Datos superaron los 60 mdp en 2022: Inai. El 28 de enero se celebra el Día Internacional de Protección de Datos Personales. Se estima que solo 2 de cada 10 empresas tienen un plan de prevención de robo de esta información. Según la Encuesta de Ciberseguridad 2022, realizada por la Asociación de Internet MX patrocinada justamente por NYCE, 22.1% de los internautas en nuestro país han sido víctimas de alguna vulneración de seguridad en los últimos 12 meses. Las principales vulnerabilidades fueron el fraude y la pérdida financiera (46.5%), la suplantación de identidad (27.3%) y el robo de información (22.2%). De hecho, el robo de identidad es uno de los incidentes delictivos directamente relacionados con la protección de datos personales. Las multas para las empresas que no cumplan con lo establecido por la ley son altas, tan solo en 2022, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai) reportó una recaudación de $60,078,958 pesos en concepto de multas por infracciones a la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP). El número de denuncias fue de 1,068 para el sector privado y 101 en el público. El Inai aseguró que, de ellas, 167 aún están tramitándose y 901 ya se dieron por concluidas en el ámbito privado. Mientras que para el público 14 aún están investigándose y 87 ya están concluidas. Asimismo, confirmó que se impusieron 119 procedimientos de sanción y se finalizaron 78, las cuales arrojaron la recaudación mencionada anteriormente." *Forbes México.* *https://www.forbes.com.mx/multas-por-infracciones-a-ley-de-proteccion-de-datos-superaron-60-mdp-en-2022-inai/*.

15.2. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) impuso en 2023 multas por un monto total de 46 millones 849 mil 777 pesos mexicanos por infracciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Los sectores más sancionados fueron los de servicios financieros y de seguros, así como el de información en medios masivos

16. **Nicaragua:** No se encontró información pública al respecto.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

17. Panamá:

17.1. **Sanciones**: ANTAI impone sanciones por violación de protección de datos." *ECO TV Panamá*, 1 de mayo de 2022, 22:57. https://www.ecotvpanama.com/politica/antai-impone-sanciones-violacion-proteccion-datos-n5717152. La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) impuso sanciones de entre mil y cuatro mil balboas a tres responsables del tratamiento de datos personales por violaciones a la Ley No. 81 de 26 de marzo de 2019 sobre Protección de Datos Personales. Las sanciones incluyeron una multa de cuatro mil balboas a un condominio por tomar fotografías de un documento de identidad sin consentimiento, tres mil balboas a una empresa por llamadas no autorizadas, y mil balboas a un medio de comunicación digital por publicar documentos personales sin permiso. Desde la entrada en vigencia de la ley en 2021, ANTAI ha tramitado 43 denuncias y ha impuesto ocho sanciones pecuniarias.

18. Paraguay: No se encontró información pública al respecto.

19. Perú:

19.1. **Multas**: Multas por infracción a la normativa en protección de datos personales pueden ascender a S/ 515,000." *EY Perú*. Contacto para prensa: Miya Mishima, Brand, Marketing & Communications Leader, EY Perú. https://www.ey.com/es_pe/law La Autoridad Nacional de Protección de Datos Personales (ANPDP) puede imponer multas de hasta S/ 515,000 a empresas por infracciones en materia de protección de datos personales, dependiendo de la gravedad de la falta. Las multas son independientes y sumatorias. Las infracciones comunes incluyen el incumplimiento en la inscripción o actualización de bancos de datos personales y la falta de publicación de una política de privacidad. Desde 2011, la normativa peruana exige cumplir con estos requisitos para evitar consecuencias jurídicas y daños a la reputación. Además de las multas, la ANPDP puede ordenar medidas correctivas para revertir la situación de vulneración.

19.2. **Multa**: Autoridad Nacional de Protección de Datos Personales impuso multas por más de S/ 7,6 millones durante el 2023." *Nota de prensa*. 14 de enero de 2024 - 9:25 a. m. https://www.gob.pe/institucion/minjus/noticias En 2023, la Autoridad Nacional de Protección de Datos Personales (ANPD) del Ministerio de Justicia y

Con el apoyo de:
Con el apoyo de:
Cooperación Española

Derechos Humanos (MINJUSDH) impuso multas por un total superior a S/ 7.6 millones. La ANPD fiscalizó a 336 entidades, tanto públicas como privadas, principalmente en los sectores financiero y de telecomunicaciones. Se iniciaron 132 procedimientos sancionadores, concluyendo 123 en primera instancia y resolviendo 33 apelaciones. Además, se archivaron 24 casos tras la subsanación de la conducta infractora por parte de los administrados. De las multas impuestas, se recaudaron S/ 2,756,695.72, cifra que es menor debido a descuentos por pronto pago, procedimientos de ejecución coactiva, y cuestionamientos en la vía contenciosa administrativa. Se emitieron 272 resoluciones sobre procedimientos trilaterales de tutela, y se inscribieron 2,670 bancos de datos personales, sumando un total histórico de 26,999. La ANPD también promovió la protección de datos personales a través de la campaña "Datito", con actividades en redes sociales y eventos, alcanzando 420 mil reproducciones en TikTok. Además, se brindaron 26 charlas informativas y se atendieron 4,081 consultas telefónicas y 1,349 por correo electrónico.

20. Portugal:

Del informe de gestión 2022[194] de la CNPD[195] se destaca lo siguiente:

- Aumentos en Ciberataques: Desde el inicio del año, hubo un notable incremento en ataques externos a sistemas de información de responsables de tratamientos de datos personales en sectores públicos y privados, lo que obligó a la CNPD a reasignar prioridades y recursos.
- Tratamiento de Datos de Ciudadanos Vulnerables: La guerra en Ucrania llevó a un urgente tratamiento de datos personales de ciudadanos extranjeros en situación de especial vulnerabilidad. También, por ello impulsaron el fortalecimiento de las infraestructuras tecnológicas y de comunicación de la CNPD.
- Sanciones y Medidas Correctivas: En 2022, la CNPD concluyó un complejo proceso de investigación técnica y jurídica, resultando en multas por infracciones relacionadas con el tratamiento de datos personales de casi toda la población, además de aplicar varias docenas de sanciones y medidas correctivas en otros procesos.

[194] Disponible en: https://www.cnpd.pt/media/tutpevyh/relato-rio_2022.pdf
[195] Los informes de gestión de la CNPD pueden consultarse en: https://www.cnpd.pt/cnpd/relatorios-de-atividades/

- Inteligencia Artificial y Reconocimiento Facial: La CNPD continuó monitoreando y orientando sobre el uso de tecnologías de IA, especialmente en el reconocimiento facial, tanto en debates públicos como en decisiones formales, publicando directrices sobre tratamientos de datos personales relacionados con comunicaciones electrónicas de marketing directo.
- Orientación sobre Retención de Metadatos: La CNPD emitió recomendaciones sobre el régimen legal de retención de metadatos y la legislación relativa al registro de pasajeros en la aviación civil.
- Adaptación de Recursos Humanos: La CNPD mantuvo una elevada carga de trabajo debido a la complejidad técnica y jurídica de los temas de protección de datos, empleando 28 trabajadores y contratando especialistas en derecho sancionador y protección de datos personales.
- Campañas de Sensibilización y Orientación: Se realizaron esfuerzos para mejorar la comunicación y procedimientos decisorios, incluyendo el desarrollo de nuevos formularios para consultas previas y aprobación de criterios de certificación.
- Incremento de Procesos: En 2022 se abrieron 2,688 procesos, un aumento de cerca de 500 procesos respecto al año anterior, destacando un significativo incremento en procesos de investigación.
- Procesos de naturaleza consultiva: En 2022, la CNPD abrió 93 procesos consultivos, lo que representa una disminución del 30% respecto al año anterior. Estos procesos incluyeron la emisión de opiniones sobre proyectos de reglamentos y protocolos administrativos, sumando un total de 63. La mayoría de estas consultas se realizaron en el marco del RGPD y la Ley n.º 59/2019, que regula el tratamiento de datos personales por autoridades competentes para la prevención y represión de delitos. Además, se abordaron temas de videovigilancia en espacios públicos. A pesar de la complejidad creciente de algunos casos, que requieren tanto análisis jurídico como pericia tecnológica, se notó la necesidad de aumentar los recursos especializados.
- Procesos de naturaleza deliberativa: La CNPD abrió 1.785 procesos de investigación en 2022, lo que representa un aumento significativo con respecto al año anterior. Estos procesos abarcan una variedad de temas, incluyendo la protección de datos personales en sectores como las comunicaciones electrónicas y el sector policial. Se realizaron 155 inspecciones, destacando auditorías a sistemas de información europeos y la inspección de datos de ciudadanos ucranianos acogidos en Portugal. Además, se abrieron 149 procesos para garantizar derechos como el acceso y la eliminación de datos en el Sistema de Información Schengen (SIS).
- En cuanto a notificaciones de violaciones de datos personales, se abrieron 367 procesos en 2022, con un aumento notable en el sector privado. Las causas principales de estas

Con el apoyo de:
Con el apoyo de:
Cooperación Española

violaciones incluyen ransomware y errores humanos. Además, la CNPD emitió 1.649 decisiones de distintos tipos, con una notable reducción respecto al año anterior debido a la necesidad de reasignar recursos a casos más complejos. Entre las sanciones aplicadas, se destacan 71 multas, principalmente por envíos de marketing no autorizados, y 57 medidas correctivas, incluyendo advertencias y órdenes para cumplir con el RGPD.

21. Uruguay:

De acuerdo con la memoria anual 2023 (Tomo I) de la Presidencia de Uruguay, la Unidad Reguladora y de Control de Datos Personales (URCDP), "en el año 2023 se iniciaron 191 expedientes, se realizaron 989 informes jurídicos de bases de datos y de expedientes iniciados, 397 informes notariales de bases de datos, se emitieron 229 resoluciones de bases de datos por el sistema, 70 resoluciones de denuncias y aprobación de transferencias internacionales, y 22 dictámenes en respuesta a consultas realizadas." (pág 190)

Adicionalmente, en dicho año la URCDP [196]:

- Continuó con el desarrollo de las líneas de acción que se han promovido en los últimos años, con el objetivo de capacitar a responsables y encargados, facilitar el cumplimiento del derecho, y atender las solicitudes de las personas, además de apoyar la consolidación de una comunidad de delegados y delegadas de protección de datos.
- Realizó diversas capacitaciones y cursos dirigidos a funcionarios públicos, además de capacitaciones específicas para delegadas y delegados, reiterándose el curso específico consistente en tres módulos especiales para ese público. Adicionalmente, se realizaron tres talleres en diversos temas como cláusulas contractuales y transferencias internacionales de datos.
- Actualizó los sistemas y herramientas para la presentación de registros de bases de datos y de solicitudes de transferencia internacional, además de las comunicaciones de vulneraciones de seguridad, para habilitar presentaciones completamente en línea y por medios seguros.

[196] Cfr. Presidencia de la República Oriental del Uruguay. Memoria anual 2023 (Tomo I). Pág. 190

Con el apoyo de:
Con el apoyo de:
Cooperación Española

22. **Venezuela:** No se encontró información pública al respecto.

Anexo 9. Viabilidad de la potencial coordinación entre los marcos normativos de los países Iberoamericanos

Es viable la coordinación entre las regulaciones de los 22 países miembros de la SEGIB siempre y cuando:

- Todos los países expidan normas generales sobre tratamiento de datos personales. Como se puso de presente en otra parte de este estudio, de los 22 países analizados, 4 no tienen normas generales sobre tratamiento de datos personales (Bolivia, Guatemala, Honduras y Venezuela). Es decir que sólo el 81,82% cuenta con NGTDP y un 18,18% carece de dicha regulación.
- Se actualicen los marcos normativos existentes, teniendo en cuenta y como referencia los documentos internacionales más recientes como, entre otros, los siguientes:
    - UE (Unión Europea) 2016. 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).
    - RIPD (Red Iberoamericana de protección de datos), 2017. Estándares de protección de datos personales para los países Iberoamericanos de la Red Iberoamericana de Protección de Datos[197].
    - OEA (Organización de Estados Americanos), 2021. Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones expedidos el 9 de abril de 2021 por el l Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA). Estos principios fueron aprobados por la Asamblea General de la OEA en noviembre de 2021.

[197] Estándares aprobados en el XV Encuentro de la RIPD, que tuvo lugar en Santiago de Chile,, el 22 de junio de 2017.

Con el apoyo de:
Con el apoyo de:
Cooperación Española

- GPA (Global Privacy Assembly), 2023. Resolución "Alcanzando estándares globales de protección de datos: principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo"
- Propuesta de actualización de la ONU (2024)
- Propuesta de una Convención Interamericana sobre Autodeterminación Informativa, Tratamiento y Circulación de Datos Personales (2024)

- Se fortalezca la cooperación entre las autoridades de protección de datos.
- Se sigan las siguientes recomendaciones de la RIPD establecidas en su plan estratégico 2021-2015[198]:

1.
Hacia un marco regulatorio de convergencia regional

1.1. Seguir impulsando los procesos regulatorios en la región, tanto en lo que se refiere a los países que aún no cuentan con normativa propia en la materia, como a los que ya disponen de ella, teniendo como marco de referencia los más recientes estándares internacionales en la materia, privilegiando especialmente los Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017. En especial, se apoyará esta adaptación a los países iberoamericanos ya adecuados al marco europeo (Argentina y Uruguay), así como a aquellos otros que acuerden poner en marcha el correspondiente proceso de adecuación ante la Comisión Europea.

1.2. Promover marcos regulatorios de alcance supranacional o regional como instrumento clave para la consolidación en la región de un modelo iberoamericano de protección de datos adaptado a las necesidades y especificidades propias de la región y de los respectivos países. Esta colaboración se estrechará con aquellas organizaciones y entidades, tanto de alcance horizontal como sectorial, que contribuyan a este objetivo de integración regional. Se tendrá especialmente en cuenta el marco de cooperación del Convenio 108 del Consejo de Europa.

198 El plan estratégico de la RIPD puede consultarse en: https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf