GOBERNANZA DE DATOS Y LAS NUEVAS TECNOLOGÍAS DE MEJORA DE LA PRIVACIDAD.

PANORAMA GLOBAL Y RETOS PARA LATINOAMÉRICA Y EL CARIBE

CONSTANZA GÓMEZ MONT • CLAUDIA DEL POZO

inai

Equipo Editorial

Edgar Samuel Rodríguez Ocampo, Kenya Soraya Martínez Ponce y María Fernanda de León Canizalez

Diseño editorial: María Alicia Barrera Aviña
Portada: Diego González Hernández

Primera versión digital, agosto 2024
ISBN: 978-607-5918-04-4
Hecho en México / *Made in Mexico*
Ejemplar de descarga gratuita

ÍNDICE

Gobernanza de Datos y las nuevas tecnologías de mejora de la privacidad.
Panorama global y retos para Latinoamérica y el Caribe
Constanza Gómez Mont y Claudia del Pozo

PRESENTACIÓN

Entre las atribuciones conferidas al **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)** se encuentra la de velar por el cumplimiento que le es debido a las autoridades de los tres niveles de gobierno, consistente en proporcionar toda información pública que le sea requerida. Aunado a lo anterior, la encomienda constitucional del INAI se encamina también a la protección de los datos personales de los ciudadanos. Ahora bien, en la actualidad el uso de tecnologías de la información, necesariamente nos obliga a vigilar su integridad y seguridad, proteger, gestionar y asegurar que la gobernanza de los datos sea siempre en apego a la norma o bien a los principios del derecho.

Las coautoras, Claudia del Pozo y Constanza Gómez Mont, son expertas en cambios tecnológicos y modelos de inteligencia colectiva. La presente obra se encuentra estructurada en torno a aspectos temáticos, primero muestran un marco conceptual en el cual desentrañan nociones y trayectos globales; después, se separan tres perspectivas sobre cómo fomentar la privacidad y gobernanza de datos: a) la regulatoria; b) la técnica y la perspectiva institucional. En cada título se pone bajo la lente el contexto en América Latina, resaltando los desafíos de la región, así como los prototipos exitosos de cada asunto.

Estamos ciertos que en todo estado democrático es imperativo hacer una defensa del acceso a la información, la labor diaria de toda institución que ejerza recurso público debe estar dotada de transparencia en el desarrollo de sus labores, además de que la defensa de la privacidad debe ser la constante para que la ciudadanía se fortalezca en un entorno de confianza y contención legal. Para todos es bien sabido el sinnúmero de consecuencias no deseadas que acarrea el indebido procesamiento y traslado de datos personales entre naciones, pues no todos los países pueden jactarse de contar con legislaciones que aseguren una real y definitiva gobernanza de datos.

En la obra se resaltan los reportes del Proyecto de Mapeo de Gobernanza de Datos Global (PMGDG) 2023, en el cual es la protección de datos uno de los elementos esenciales que deben tomar en cuenta el sector encargado de formular las políticas públicas en el mundo, además de la gobernanza de los datos que generan información a través de la inteligencia artificial (IA).

Las autoras con gran conocimiento del tema muestran la evolución normativa internacional en torno a la protección de la privacidad

en los flujos transfronterizos de los datos personales, la cual puede entenderse desde finales del siglo XX con el auge del internet, hasta finales de 2023 con regulaciones emitidas por la Unión Europea en materia de Reglamento de Datos.

El inminente y acelerado crecimiento en el uso de las tecnologías de la información y la digitalización de las sociedades ha acarreado consigo la gran carga a los Estados de garantizar el derecho fundamental de protección a los datos personales, así como su uso responsable por los actores del estado y los particulares, creando con ello políticas públicas y económicas globales.

Las autoras y su equipo exponen ampliamente los avances en la región de América Latina en materia de protección de datos, que incluso han sido materia de análisis internacional, pues con ello se ha coadyuvado en la creación de modelos y leyes que tutelen la creación, el desarrollo y la actualización de la regulación nacional en la materia. Sin lugar a duda, los países latinoamericanos cuentan con la experiencia de los pares más avanzados en la materia, para poder construir normas e instituciones que sirvan de ejemplo y experiencia de casos de éxito para formar estructuras sólidas en materia de protección y gobernanza de datos.

Apreciados lectores, continuamos propiciando la creación y distribución de las obras editoriales emanadas desde el Comité Editorial. Entendemos que este tipo de libros son elementos indispensables de difusión de la cultura de los derechos que en el instituto se tutelan y estamos ciertos de que serán de mucha utilidad para la sociedad en general como para los especialistas o estudiosos de la materia. Los invitamos a adentrarse en el apasionante mundo del derecho comparado desde la perspectiva de dos especialistas.

Comité Editorial del INAI

ACERCA DE LAS AUTORAS

Constanza Gómez Mont

Fundadora de *C Minds*, trabaja en el campo de las tecnologías emergentes para el bien social y ambiental, colaborando con socios como el BID, el gobierno del Reino Unido, la UICN, GIZ, UNESCO, entre otros. También es fundadora de *AI for Climate* y líder de *NaturaTech LAC*, una iniciativa global nacida en 2024 para acelerar el uso de nuevas tecnologías para la conservación de la biodiversidad en la región LAC. Además, es miembro del comité directivo de la plataforma global *Women for Ethical AI* de la UNESCO, expresidenta del *GFC AI for Humanity* del Foro Económico Mundial (WEF) y nombrada *Yale Climate Fellow 2024*.

Ha liderado diversos procesos globales de alto nivel, como el co-desarrollo del primer instrumento regulatorio global de ética de la IA, liderado por la UNESCO, firmado por 193 países; la presidencia del Consejo del Futuro Global de IA para la Humanidad del Foro Económico Mundial. Es miembro fundador del consejo global de Mujeres por la IA Ética de la UNESCO, entre otros roles de liderazgo. Es asesora y socia de gobiernos, organizaciones multilaterales y grandes empresas tecnológicas. Ha sido reconocida por el Gobierno Británico como Líder Internacional, ganó el Premio *AI Life Trajectory Award* de Norteamérica 2023 por Mujeres en IA, y es *Climate Fellow* de la Universidad de Yale 2024, entre otros reconocimientos. Aboga y habla activamente sobre el liderazgo inclusivo, el empoderamiento de las mujeres y el uso ético de la tecnología para el impacto.

Claudia del Pozo

Fundadora y Directora de *Eon Institute*, un *think-tank* mexicano liderado por mujeres que impulsa una sociedad a prueba de futuro ante los cambios tecnológicos (*spin-off* independiente de *C Minds*, una organización que ayudó a crear). Su trabajo la ha llevado a ser seleccionada para ser parte del Consejo de Expertos de la Alianza Nacional de IA del Senado de la República de México y unirse al Consejo Consultivo de Tecnologías Emergentes del Reino Unido en México. En el pasado, coordinó el primer prototipo de políticas públicas (tipo *sandbox*) para sistemas de IA más responsables en México, así como un ejercicio similar en Uruguay enfocado en Tecnologías que Protegen la Privacidad (PETs).

En el 2024, fue destacada por WIRED en español como una de las mujeres principales en proteger a Latinoamérica de los riesgos de la IA. En 2022 fue reconocida como componente clave del ecosistema mexicano por los *Women in AI Awards* además de ser finalista de la categoría Líder de IA responsable. Su trabajo en IA responsable y otras tecnologías emergentes desde *Eon Institute* ha sido compartido en programas, foros y revistas locales e internacionales como *Bloomberg BusinessWeek, Forbes, WIRED, MIT Sloan Business Review*, Excélsior, El Financiero y Radio Chilango por mencionar algunos. Es graduada de negocios de la *Warwick Business School* en el Reino Unido y empezó su carrera en IBM Alemania.

ÍNDICE DE ABREVIATURAS

Abreviatura	Significado
AGESIC	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento
AGETIC	Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación de Bolivia
BID	Banco Interamericano de Desarrollo
CCPA	Ley de Protección de Consumidores de California
CEPAL	Comisión Económica para América Latina y el Caribe
CPPA	Agencia de Protección de Privacidad de California
CPRA	Ley de Derechos de Privacidad de California
DGA	Ley de Gobernanza de Datos de la Unión Europea
DMA	Regulación de Mercados Digitales de la Unión Europea
DPAs	Autoridades de Protección de Datos
DSA	Regulación de Servicios Digitales
ENDE	Estrategias Nacionales para el Desarrollo de las Estadísticas
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
GPAI	Alianza Global sobre Inteligencia Artificial
IA	Inteligencia Artificial
ICO	Oficina del Comisionado de Información
ILDA	Iniciativa Latinoamericana por los Datos Abiertos
IMDA	Autoridad de Desarrollo de Comunicaciones
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
IoT	Internet de las Cosas
LFDPPP	Ley Federal de Protección de Datos Personales en Posesión de Particulares
LGPD	Ley General de Protección de Datos Personales de Brasil
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
NIST	Instituto Nacional de Estándares y Tecnología
NSF	Fundación Nacional de Ciencias
ONE	Oficinas Nacionales de Estadística
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ONU	Organización de las Naciones Unidas
PbD	Privacidad desde el Diseño
PETs	Tecnologías que Preservan la Privacidad
PMGDG	Proyecto de Mapeo de Gobernanza de Datos Global
PPDSA	Estrategia Nacional para Promover la Analítica y Transferencia de Datos Protegiendo la Privacidad
PyMEs	Pequeñas y medianas empresas

RACSEL	Red Americana de Cooperación sobre Salud Electrónica
RGPD	Reglamento General de Protección de Datos
SMPC	Computación Multipartita Segura
TEE	Entorno de Ejecución de Confianza
TI	Tecnologías de la Información
UE	Unión Europea
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
URCDP	Unidad Reguladora y de Control de Datos Personales
WDR	Reporte de Desarrollo Global

INTRODUCCIÓN

La privacidad y la gobernanza de datos se sitúan en el epicentro de debates a nivel global y local al abordar cómo las tecnologías pueden impulsar el crecimiento social y económico. Esta temática, aunque no es nueva en el diálogo tecnológico, cobró especial atención en 2018, a raíz de la evidencia de filtraciones significativas y usos indebidos de datos que pusieron en riesgo los fundamentos democráticos. A esto se suma la intensificación del uso de la inteligencia artificial (IA) generativa entrenada con millones de datos disponibles sin que se conozca con exactitud si estos han sido legítimamente recolectados y/o tratados. Hoy día, las interrogantes sobre el acceso, precisión, compartición y protección de datos resultan cruciales en una sociedad cuya interacción con la tecnología es cada vez mayor.

Este reporte tiene como propósito brindar claridad en cuanto a la gobernanza y privacidad de datos en el actual escenario tecnológico, enfocándose en cómo estas cuestiones han evolucionado en el ámbito público. Mientras que la privacidad de datos tiene que ver con el correcto almacenamiento, acceso, conservación, inmutabilidad y seguridad de los datos sensibles (Bigelow, 2022), la gobernanza de datos se refiere al proceso de gestión de la disponibilidad, facilidad de uso, integridad y seguridad de los datos en los sistemas de una entidad (Stedman y Vaughan, s.f.).

El documento se estructura en secciones clave que tratan diversos aspectos de la temática. Se inicia con un marco contextual que esclarece conceptos y trayectorias, seguido por un análisis de tendencias y avances globales en privacidad y gobernanza de datos. Posteriormente, se desgranan tres perspectivas sobre cómo fomentar la privacidad y gobernanza de datos: la regulatoria (donde se esbozan mejores prácticas y retos); la técnica (resaltando las tecnologías que preservan la privacidad (PETs) como el cifrado y la anonimización) y, finalmente, la perspectiva institucional. En cada sección, se pone bajo la lupa la situación en América Latina, subrayando los retos únicos de la región y ejemplos exitosos relacionados con cada temática.

En el contexto institucional, el reto es aún mayor, ya que los Estados deben observar y salvaguardar el principio de transparencia como forma democrática para tener acceso a información, y establecer marcos regulatorios suficientes para proteger la privacidad en su mayor extensión, lo cual invariablemente debe reflejarse en la construcción de un entorno de confianza. Las naciones que adoptan un enfoque integral estructuran estrategias, políticas, procesos, y adaptan instrumentos orga-

nizacionales para regular distintos escenarios, tipos y contextos de uso de datos. Las instituciones capaces de anticiparse a estos cambios tienen mayores probabilidades de cumplir con las expectativas legales y éticas que las personas depositan en ellas para la protección de sus datos.

Con este informe, se aspira a ofrecer un recurso para quienes estén interesados en el tema, así como para autoridades y profesionales en América Latina dedicados a la protección y gobernanza de datos, ofreciéndoles mejores prácticas internacionales que puedan informar avances en la región. Asimismo, se pretende enriquecer el debate global sobre privacidad y gobernanza de datos impulsando la armonización de la regulación de la innovación tecnológica con una perspectiva de respeto a los derechos fundamentales desde una óptica regional.

PANORAMA GLOBAL

Esta sección se enfoca en explorar mejores prácticas internacionales en la materia de gobernanza de datos. Se destacan enfoques que puedan orientar las conversaciones e inspirar acciones en países que están explorando cómo abordar de manera más efectiva este tema.

El resumen de los reportes del Proyecto de mapeo de gobernanza de datos global (PMGDG) de 2023, en inglés *Global Data Governance Mapping Project* (Strutt et al., 2023), destaca la protección de datos como una de las principales preocupaciones de las personas formuladoras de política pública alrededor del mundo, junto con la gobernanza de sistemas impulsados por los datos como la IA. Además de notar una discrepancia entre la cantidad de acciones tomadas para la gobernanza de los datos entre los países de altos y bajos ingresos, el reporte también encuentra una diferencia en enfoques: los países de menores ingresos priorizan enfoques estructurales y regulatorios, mientras que los países de mayores ingresos prefieren desarrollar estrategias o priorizar lineamientos éticos y centrados en los derechos humanos. De forma general, también se observó que las personas formuladoras de política pública tienden a prestar escasa atención y consideración a las preocupaciones del público en la temática.

El reporte también destaca una tendencia hacia el enfoque en normas que regulan tecnologías específicas en lugar de normas que regulan los datos como entrada para dichas tecnologías. Existe la preocupación de que, sin reglas específicas para gobernar los datos, los países podrían ser incapaces de responder de manera efectiva a los diversos y complejos usos de los datos.

A nivel global de los países más avanzados en temas de gobernanza de datos en los últimos tres años, según un estudio del PMGDG, se encuentran Reino Unido, Australia, Francia y Nueva Zelanda, mientras que Egipto, Argelia, Botsuana, Cuba e Irán se encuentran entre los últimos de la lista. El recuadro a continuación explora la temática en América Latina.

Perspectiva desde América Latina y el Caribe

El Proyecto de mapeo de gobernanza de datos global (PMGDG) evalúa el avance de distintos países en cuanto a gobernanza de datos, vía una puntuación basada en seis categorías, cada una con indicadores clave que se presentan a continuación:

» **Indicadores de estrategia** (se trata de saber si el país cuenta con los siguientes indicadores): Estrategia Nacional de Datos, Estrategia de Administración Pública, Estrategia de IA, Estrategia para los Datos del Ecosistema Digital;

» **Indicadores regulatorios** (se trata de saber si el país cuenta con los siguientes indicadores): Ley de protección de datos personales, Ley de datos abiertos para la publicación proactiva de información gubernamental, Acta de Libertad de Información, Derecho a ser protegido por la toma de decisión autónoma, Derecho de portabilidad de datos;

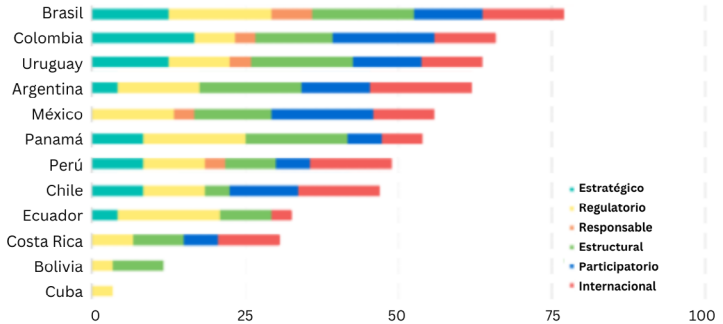
» **Indicadores de responsabilidad** (se trata de saber si el país cuenta con los siguientes indicadores): Carta internacional de datos abiertos, Marco de ética de los datos en el sector público, Iniciativas de IA responsable, Marcos de confianza para la gestión de la identidad digital, Lineamientos para la transferencia de datos no gubernamentales;

» **Indicadores estructurales** (se trata de saber si el país cuenta con los siguientes indicadores): Organismo de protección de datos personales, Portal de datos abiertos, Organismo de coordinación de datos abiertos, Organismo de gobernanza de datos del sector público;

» **Indicadores participativos** (se trata de saber si el país cuenta con los siguientes indicadores): Consultas públicas sobre los datos, Respuesta gubernamental a las consultas, Órgano asesor de múltiples partes interesadas;

» **Indicadores internacionales** (se trata de saber si el país ha firmado o ratificado los siguientes indicadores): Convención 108+, Alianza de Gobierno Abierto, Principios de IA de la OCDE, Acuerdos comerciales vinculantes sobre el flujo transfronterizo de datos, Convención de Budapest.

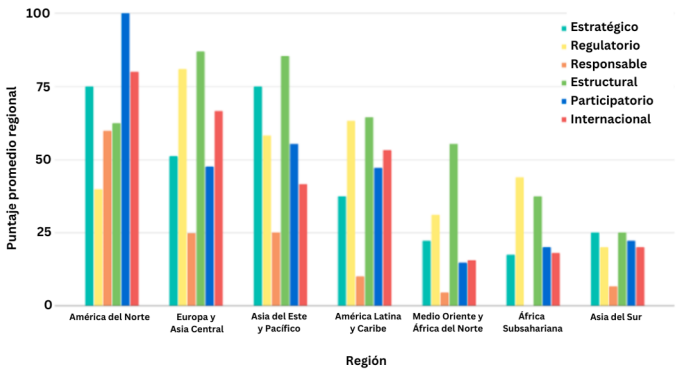
De acuerdo con el Proyecto de mapeo de gobernanza de datos global (PMGDG), los países latinoamericanos se encuentran en una posición promedio de 34.4 en materia de gobernanza de datos, posicionando a la región por debajo del promedio entre 69 países. Entre los países incluidos se encuentran Brasil (posición 7 de 69), Colombia (19), Uruguay (20), Argentina (21), México[1] (25), Panamá (27), Perú (31), Chile (35), Ecuador (47), Costa Rica (49), Bolivia (63) y Cuba (68). Se pueden ver los puntajes en cada dimensión en la gráfica resumida a continuación.



Gráfica 1 - Puntaje promedio final de los países de América Latina en el mapeo de gobernanza de datos global (PMGDG, 2023).

De forma general se puede observar que la región está rezagada en temas de responsabilidad que incluye contar con una carta de datos, un marco ético de datos para el sector público, iniciativas de IA responsable, un marco de confianza para la gestión de la identidad digital y lineamientos para el intercambio no-gubernamental de datos. Esta dimensión suele ser la menos desarrollada por país, como se muestra en la gráfica por región a continuación.

1 Vale la pena mencionar que este análisis considera que México no tiene Estrategia de Inteligencia Artificial, por lo que el país tiene un puntaje de cero en la dimensión estratégica. En realidad, México desarrolló una estrategia nacional de IA bajo una administración anterior, realizada por la Embajada Británica en México, C Minds y el Open Data Institute. Sin embargo, la nueva administración no le dio continuidad, como fue el caso en Argentina. Esta fue aceptada por la Presidencia de la República en 2018. (Presidencia de la República, 2018).



Gráfica 2 - Puntajes promedios regionales (PNGDG, 2023).

Si bien la región de América Latina y el Caribe obtiene mejores puntajes generales que el Medio Oriente y África del Norte, África Subsahariana y Asia del Sur, todavía falta impulsar el tema de gobernanza de datos, ya que los países no cuentan con marco de ética de datos en el sector público, ni marco de confianza para la gestión de la identidad digital, ni lineamientos de datos para el intercambio no-gubernamental de datos.

Es esencial abordar la privacidad de datos y la gobernanza en diversos contextos, como América Latina, el Caribe, la Unión Europea y Estados Unidos. Esto permite comprender y analizar las tendencias globales en estas áreas, para poder comparar lo que están realizando países más avanzados en la materia contra los países que están empezando a ver estos temas y poder facilitar el establecimiento de normativas y prácticas comunes para resguardar la información personal.

A pesar de las variaciones en regulaciones, la creciente interconexión mundial destaca la importancia de homologar políticas de protección. Esta convergencia no solo refuerza la seguridad, sino que también contribuye a construir una confianza más sólida entre regiones. Las siguientes secciones se centran en diferentes enfoques complementarios que se pueden tomar en cuenta para una gobernanza y privacidad óptimas de los datos.

ENFOQUES REGULATORIOS

A pesar de que se piensa que la protección y gobernanza de datos llegó con el auge del internet, es una discusión que se ha tenido desde finales del siglo XX. De hecho, el estado de Hesse en Alemania fue el primer gobierno que introdujo la primera legislación de protección de datos del mundo en 1970, llamada "Datenschutzgesetz" (DSG; ley de protección de datos). Esta ley fue seguida por legislaciones similares en diferentes países y posteriormente adoptada a nivel nacional en Alemania en 1977 (GDPR Hub, s.f.).

Asimismo, en los años 80, la Organización para la Cooperación y el Desarrollo Económico (OCDE) estableció las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980), que tienen como objetivo establecer un consenso internacional sobre las pautas generales para la recopilación y gestión de información personal, facilitando las transferencias internacionales de datos de una forma que respete los derechos humanos. Estas directrices podían incorporarse a las leyes existentes o servir de base para nuevas legislaciones, ya que se crearon de forma flexible y con una formulación que permitía adaptarlas a los cambios tecnológicos.

Caja 1. Principios de las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE

Los principios incluyen:

1. Limitar la recopilación de datos personales de manera legal y justa;
2. garantizar la calidad y relevancia de los datos para los fines para los que se van a utilizar;
3. especificar para qué fines se recopilan y usan los datos personales;
4. restringir su uso para esos fines específicos;
5. implementar las mejores prácticas de medidas de seguridad;
6. promover la transparencia en las prácticas de datos;
7. permitir la participación y los derechos de acceso y corrección de datos personales por parte de los individuos; y

8. responsabilizar al responsable del tratamiento de datos por el cumplimiento de estos principios.

A partir de estos primeros esfuerzos, las regulaciones de privacidad de datos se fueron expandiendo a nivel mundial. El Convenio 18 (Parlamento Europeo, s.f.), conocido como la "Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", fue el primer instrumento legalmente vinculante a nivel internacional. Fue diseñado por el Consejo de Europa para salvaguardar los derechos de privacidad y protección de datos de las personas en el contexto del procesamiento automatizado de datos personales y entró en vigor en 1985. Entre los principios clave figuran el principio de limitación de la finalidad, los principios de calidad de los datos, la transparencia, los derechos de acceso, rectificación y oposición, y el establecimiento de autoridades de supervisión independientes para garantizar el cumplimiento del convenio.

A pesar del auge tecnológico a principios de los 2000 y la llegada de la banca en línea en las entidades financieras, el lanzamiento de Facebook en 2006 y la demanda hacia Google por escanear correos electrónicos de sus usuarios en 2011 (Reglamento General de Protección de Datos [RGPD], s.f.) que apuntaban hacia la necesidad de actualizar y fortalecer las regulaciones existentes, estas no recibieron muchas modificaciones.

Fue en 2018 que el Convenio 108 (llamado ahora convenio 108+) fue modernizado según el Consejo Europeo (s.f.) para *"adaptar este instrumento a las nuevas realidades y al mundo cada vez más conectado y fortalecer su implementación efectiva"*, con el objetivo de mantener un equilibrio entre la promoción de los flujos informativos como impulsores de la comunicación, la economía, la apertura e incluso la democracia, y los valores fundamentales de respeto a la privacidad y protección de datos personales. A la fecha del 2021, el Convenio 108 había sido ratificado por 55 países y en 2023 sigue desempeñando un papel crucial en la promoción y protección de los derechos a la privacidad y la protección de datos en un mundo cada vez más interconectado e impulsado por los datos.

El año que marcó la transición a un mundo más enfocado en la protección de los datos fue el 2016, cuando la Unión Europea (UE) lanzó la primera regulación integral en materia de protección y gobernanza de datos: la Regulación General de Protección de Datos, más conocida como RGDP, presentada a continuación en la Tabla 1.

Caja 2. La Regulación General de Protección de Datos de la Unión Europea

La RGPD surge como propuesta nueva en la UE el 2012, después de una consulta pública sobre protección de datos promovida por la Comisión Europea en el 2009, considerando los escasos cambios en la legislación europea relacionada a datos personales desde los 90.

En 2016, la UE adoptó la RGPD, el cual es un marco jurídico cuyo objetivo es proteger los datos personales y la privacidad de los ciudadanos de la UE. Esta ley busca armonizar las leyes de privacidad de datos en toda Europa; proteger y potenciar la privacidad de los datos de todos los ciudadanos de la UE y reformar la manera en que las organizaciones de toda la región abordan la privacidad de los datos.

Esta ley afecta a las empresas que manejan datos de ciudadanos de la UE, incluidos bancos y compañías de seguros, entre otros. Establece los derechos de las personas y las obligaciones de las empresas, incluida la protección de los datos personales cuando se exportan fuera de la UE (Rossow, 2018).

En el corazón del RGPD se encuentran principios fundamentales, creados para guiar el procesamiento de datos personales, no como reglas estrictas (Burges, 2020). Son siete en total (RGPD, s.f.):

» **Legalidad, equidad y transparencia:** El manejo de los datos debe ser legal, honesto y transparente para la persona sujeta a los datos.

» **Delimitación de la finalidad:** Se deben utilizar los datos con fines legítimos y específicos, previamente comunicados de manera clara a la persona sujeta a los datos al momento de recopilarlos.

» **Minimización de datos:** Los datos personales deben ser apropiados, relevantes y limitados con relación a la finalidad con los que se utilicen.

» **Exactitud:** Se deben de mantener los datos personales precisos y actualizados.

» **Limitación del plazo de conservación:** Únicamente se pueden retener datos de identificación personal durante el período necesario para el propósito específico establecido.

» **Integridad y confidencialidad (seguridad):** El tratamiento de los datos debe realizarse de forma que se garantice la seguridad adecuada (por ejemplo, mediante el uso de encriptado).

» **Rendición de cuentas:** La persona responsable del tratamiento de los datos tiene la responsabilidad de demostrar el cumplimiento de todos los principios de la RGPD.

En gran medida, estos principios son similares a los que existían en leyes anteriores de protección de datos (Burges, 2020), con excepción al principio de responsabilidad (British Council, s.f.).

Del otro lado del Atlántico, Estados Unidos tomó un camino diferente sobre el tema. En la actualidad, el país no cuenta con una ley general que regule la recopilación, protección y privacidad de datos, sino más bien con un sistema de leyes a nivel federal y estatal que regulan sectores y tipos específicos de información personal. Estas leyes responden a acrónimos como HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA y VPPA (Klosowski, 2021). En comparación a la UE, la falta de un enfoque centralizado significa que muchas empresas no tienen restricciones en cuanto al uso y tratamiento de los datos.

A su vez, después del lanzamiento de RGPD, el estado estadounidense de California decidió inspirarse en el documento para diseñar la Ley de Protección de Consumidores de California, conocida como CCPA por sus siglas en inglés, resumida en la Caja 3.

Caja 3. La Ley de Protección de Consumidores de California (CCPA)

En 2018, California se convirtió en el primer estado de Estados Unidos en promulgar una ley integral de privacidad de datos para las personas consumidoras conocida como la CCPA. Esta ley otorga a residentes de California una amplia gama de derechos en relación con la recopilación, uso, almacenamiento y compartición de su información personal por parte de las empresas cubiertas (Stockburger, 2022), por ejemplo:

» Derecho a conocer la información personal que una empresa recopila sobre las personas consumidoras y cómo se utiliza y comparte;

» El derecho a eliminar la información personal que se recopile (con algunas excepciones);

» El derecho a optar por no vender o compartir su información personal; y

» El derecho a no ser discriminado por ejercer sus derechos en virtud de la CCPA.

La CCPA entró en vigor el 1 de enero de 2020 y en noviembre de 2020, los votantes de California aprobaron la Proposición 24, la CPRA, que modificó la CCPA y añadió nuevas protecciones adicionales de la privacidad que comenzaron a aplicarse el 1 de enero de 2023. La CCPA amplió los derechos y la flexibilidad de los residentes de California en cuanto al control de su información personal, y la Agencia de Protección de Privacidad de California (California Privacy Protection Agency, CPPA) se volvió la nueva agencia encargada de hacer cumplir la Ley de Derechos de Privacidad de California (California Privacy Rights Act, CPRA) junto con el Fiscal General de California. Dentro de estos nuevos derechos se encuentran (State of California Department of Justice, 2023):

» El derecho a corregir la información personal inexacta que una empresa tenga sobre las personas consumidoras; y

» El derecho a limitar el uso y la divulgación de la información personal sensible que se recopile sobre estas personas.

Existe una gran variedad de empresas sujetas al CCPA (incluyendo los intermediarios), las cuales tienen la responsabilidad de responder a las solicitudes de las personas consumidoras, ejercer sus derechos y facilitar la información sobre las prácticas de privacidad de las empresas.

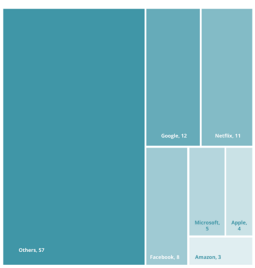
Las leyes RGPD y CCPA comparten similitudes en términos de la definición de ciertos conceptos que aunque no los ponen con los mismos nombres, es la misma definición (Ternullo, 2019) (por ejemplo, datos personales vs información personal, responsable del tratamiento de datos vs empresas y, encargado del tratamiento vs proveedor de servicios), la implementación de protecciones adicionales para menores de 16 años, la garantía de derechos de acceso a la información personal, además ambas leyes aplican a empresas con sede fuera de sus respectivas jurisdicciones y cuentan con principios en común como el derecho a la eliminación de datos o el derecho de oposición (Bateman, 2023).

Estos avances han provocado que cada vez más países promulguen leyes de protección y gobernanza de datos. Según la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2021) o UNCTAD por sus siglas en inglés, en 2021, 137 de 194 países habían promulgado leyes en la materia. Para mediados de marzo de 2022, subió la cifra a 157 países (Greenleaf, 2022). Estas leyes en su mayoría han estado influenciadas principalmente por la RGPD, aunque con muchas variaciones en sus implementaciones. De hecho, en el 2022, únicamente 17 países contaban con iniciativas o leyes de privacidad que podían ser comparables al RGPD (Simmons, 2022): Australia, Brasil, Canadá, Chile, China, Corea del Sur, Egipto, India, Israel, Japón, Nueva Zelanda, Nigeria, Sudáfrica Suiza, Tailandia, Turquía y Estados Unidos (únicamente con la Ley de Privacidad del Consumidor de California, CCPA) (Robichaud, 2020).

Desde entonces, la RGPD ha sido complementada con otras regulaciones que agregan especificaciones y se adecúan cada vez más a los avances en desarrollo tecnológico. En 20202, la UE pasó otra regulación innovadora: La Regulación de Mercados Digitales de la Unión Europea (DMA, por sus siglas en inglés), enfocada en prácticas digitales que aún no estaban reguladas para promover mercados justos y más abiertos (Comisión Europea, s.f. a), presentada a continuación.

Caja 4. Ley de Regulación de Mercados Digitales de la Unión Europea (DMA)

La UE aprobó un nuevo Reglamento de Mercados Digitales (DMA) el 14 de septiembre de 2022, con el objetivo de poner fin al dominio de los gigantes de Internet, considerando el monopolio virtual que tienen en el mercado europeo. El Área de Mercados Digitales pretende imponer normas que beneficien a las empresas europeas y a los internautas. La siguiente gráfica demuestra dicho monopolio.



Gráfica 3. Parte del tráfico mundial de Internet por empresa en 2018 (% del total) (Sandvine, 2019 en Banco Mundial, 2021).

El Reglamento se dirige a 10 "servicios esenciales de plataforma" o servicios básicos que son considerados problemáticos en la actualidad, entre ellos los motores de búsqueda, las redes sociales o servicios en la nube.

La normativa solo afecta a las empresas que son "controladores de acceso" o guardianes (*gatekeepers*) de la entrada de Internet. Se definen como empresas que:

» gozan de una sólida posición económica, tiene un impacto significativo en el mercado interior y operan en varios países de la Unión Europea;

» tienen una posición de intermediación fuerte, lo que significa que conecta a una gran base de usuarios con un gran número de empresas;

» tienen (o están cerca de tener) una posición de mercado fuerte y sostenible, lo que significa que es estable a lo largo del tiempo.

Las empresas que cumplían estos criterios tenían que registrarse en la Comisión Europea, que las designaría oficialmente como controladores de acceso el 6 de septiembre de 2023. También designó como controladores de acceso a empresas que no alcanzaran todos estos umbrales, pero que se consideraran lo suficientemente dominantes, en función a determinados criterios.

Las empresas designadas como controladores de acceso deberán designar a una o varias personas responsables del cumplimiento del reglamento y cumplir una veintena de obligaciones o prohibiciones antes del 6 de marzo de 2024, para cada uno de sus servicios esenciales de plataforma. En temas de gobernanza y privacidad de datos, por ejemplo, tendrán que permitir a empresas usuarias acceder a los datos generados por sus actividades en su plataforma y no podrán reutilizar los datos personales de un usuario con fines de publicidad dirigida sin su consentimiento explícito. (Comisión Europea, s.f. a).

Las reformas de la UE sobre el uso de datos personales no terminan con la DMA. En agosto de 2023 entró en vigor la Regulación de Servicios Digitales, conocido como DSA, por sus siglas en inglés. La siguiente tabla resume los objetivos y el alcance de este reglamento.

Caja 5. Ley de Regulación de Servicios Digitales de la Unión Europea (DSA)

La DSA establece, por primera vez, un conjunto común de reglas sobre las obligaciones y responsabilidades de los intermediarios en todo el mercado único que abrirá nuevas oportunidades para ofrecer servicios digitales a través de fronteras, garantizando al mismo tiempo un alto nivel de protección para todas las personas usuarias, sin importar dónde residan en la UE (Comisión Europea, s.f. b).

Las obligaciones de los diferentes actores en línea corresponden con su rol, tamaño e impacto en el ecosistema en línea para fomentar la innovación, el crecimiento y la competitividad, y facilitar la expansión de plataformas más limitadas, pequeñas y medianas empresas (PyMEs) y startups. Las responsabilidades de las personas usuarias, plataformas y autoridades se re-equilibran de acuerdo con los valores europeos, colocando a la ciudadanía en el centro. Las reglas:

» **Mejoran la protección** de las y los consumidores y sus derechos fundamentales en línea

» **Establecen un marco de transparencia** poderoso y una clara responsabilidad para las plataformas en línea

» **Fomentan la innovación, el crecimiento y la competitividad** dentro del mercado único.

Por otro lado, la Ley de Gobernanza de Datos de la Unión Europea (DGA, por sus siglas en inglés) tomó efecto en septiembre de 2023, y establece una serie de reglas para promover el acceso a datos del sector público para el desarrollo de nuevos productos y servicios y le permite más control a las personas sobre sus datos personales, ofreciéndoles herramientas para gestionar la forma en que se accede a su información (Irwin, 2022). Se puede leer más acerca de dicha regulación en la siguiente tabla.

Caja 6. Ley de Gobernanza de Datos de la Unión Europea (DGA)

El Consejo Europeo aprobó en mayo de 2022 la Ley de Gobernanza de Datos, en línea con la aprobación previa del Parlamento Europeo. Esta regulación sobre gobernanza de datos entró en vigor el 23 de junio de

2022 y, después de un período de gracia de 15 meses, comenzó a ser aplicable a partir de septiembre de 2023 (Comisión Europea, 2023 a).

Esta ley tiene como objetivo promover la disponibilidad de datos y crear un entorno confiable para su uso en investigación y desarrollo de nuevos servicios y productos innovadores. Esta ley busca aumentar la confianza en el intercambio de datos, superar obstáculos técnicos y fomentar la reutilización de datos. También respalda la creación de espacios de datos europeos comunes en sectores estratégicos (Comisión Europea, 2023 a), por ejemplo, en sectores económicos, mejores políticas públicas y una gobernanza más transparente. Además, el uso de datos en áreas como la salud, movilidad, medio ambiente, agricultura y administración pública conlleva beneficios significativos, como tratamientos médicos personalizados, transporte más eficiente, acciones contra el cambio climático y avances en el desarrollo agrícola (Comisión Europea, 2023 a).

Para eso se implementará una certificación opcional con el fin de identificar a los proveedores de servicios de intermediación de datos y organizaciones de gestión de datos, con fines altruistas que cumplan con los requisitos establecidos (Consejo Europeo, 2022). Adicionalmente, se establecerá el Comité Europeo de Innovación en Datos, el cual tendrá la responsabilidad de brindar asesoramiento y apoyo para mejorar la interoperabilidad de los servicios de intermediación de datos, así como ofrecer directrices para el desarrollo de espacios de datos.

La Ley de Gobernanza de Datos establece protecciones para los datos del sector público, los servicios de intermedios de datos y las organizaciones sin fines de lucro que manejan datos, en relación con la transferencia ilegal de datos no personales a nivel internacional y el acceso no autorizado del gobierno a dichos datos (Consejo Europeo, 2022). En lo que respecta a los datos personales, la UE ya cuenta con garantías similares bajo el RGPD.

En resumen, la Ley de Gobernanza de Datos busca promover la disponibilidad y el uso seguro de los datos en beneficio de la investigación, la innovación y la sociedad en general.

Si bien la DGA crea los procesos y estructuras para facilitar los datos, todavía faltaba definir quién puede crear valor a partir de los datos y bajo qué condiciones. Para responder a esta necesidad, la UE generó el Reglamento de Datos que busca garantizar justicia a través de normas relativas al uso de los datos generados por los dispositivos del Internet de

las Cosas. En noviembre de 2023, tanto el Parlamento Europeo como el Consejo de la Unión Europea aprobaron la regulación (Comisión Europea, 2023). Se puede leer más acerca de esta disposición en la siguiente tabla.

Caja 7. Reglamento de Datos de la Unión Europea

Aprobado en noviembre de 2023, este reglamento tiene como objetivo garantizar la equidad en la asignación del valor de los datos entre los agentes del entorno digital; estimular un mercado de datos competitivo; generar posibilidades para la innovación basada en los datos; y hacer que los datos sean más accesibles para todos (Consejo Europeo, 2023). Se prevé que el Reglamento tenga un gran impacto en quienes gestionan datos, tanto personales como impersonales, de personas usuarias de productos y servicios conectados. Especialmente cuando los datos provienen de productos o servicios relacionados con el Internet de las Cosas (IoT, por sus siglas en inglés).

Concretamente el reglamento propone:

» **Acciones** para permitir que las personas usuarias de dispositivos conectados accedan a los datos generados por esos dispositivos y los servicios asociados. Sobre IoT, se centra en las funcionalidades de los datos de productor conectados, diferenciando "datos de producto" de "datos de servicios relacionados".

» **Disposiciones** para fomentar el intercambio de datos al mismo tiempo que se garantiza la protección de secretos comerciales y derechos de propiedad industrial y salvaguardias contra comportamientos abusivos.

» **Medidas** para evitar cláusulas contractuales abusivas impuestas unilateralmente, protegiendo a las empresas de la UE y fomentando negociaciones justas, especialmente para las PyMEs en el mercado digital.

» **Métodos** para que las entidades gubernamentales accedan a datos del sector privado en situaciones de emergencia pública o cumplimiento de mandatos legales cuando esos datos no estén fácilmente disponibles por otras vías.

» **Nuevas normas** que permiten a los clientes cambiar libremente entre diferentes proveedores de servicios de procesa-

miento de datos en la nube, promoviendo la competencia y evitando la dependencia de un único proveedor. Además, se han incluido medidas de protección contra transferencias no autorizadas de datos.

» **Acciones** para fomentar el desarrollo de estándares de interoperabilidad que faciliten el intercambio y procesamiento de datos, en línea con la Estrategia de Normalización de la UE.

El acuerdo político logrado entre el Parlamento Europeo y el Consejo entró en vigor 20 días después de ser publicado en el Diario Oficial de la Unión Europea y se aplicará en su totalidad 32 meses después, con excepciones para ciertas obligaciones de acceso a datos de productos conectados y servicios relacionados.

Actualmente, y tras una revisión de los resultados de la aplicación de la RGPD, la UE encontró áreas de oportunidad, en particular en cuanto a mecanismos de colaboración entre países miembros, por lo que está explorando la posibilidad de publicar reglas procedurales adicionales en el tema (Comisión Europea, 2023 b).

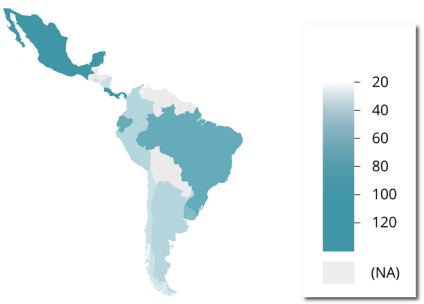
En conclusión, gran parte de los países están actualizando y generando nueva regulación en materia de protección y gobernanza de datos, destacando el compromiso global por abordar de manera efectiva los desafíos de la privacidad actuales, pero la región que lidera el tema regulatorio sin duda es la UE que ofrece un modelo de regulación gradual interesante. Dicho esto, América Latina y el Caribe están presentando grandes avances, como se presenta en la sección a continuación.

Perspectiva desde América Latina y el Caribe

Existen varios países en la región con leyes de protección de datos personales vigentes: Argentina, Bahamas, Barbados (The Barbados Parliament, 2019), Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Jamaica (Data Guidance, 2023), México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Trinidad y Tobago y Uruguay (Red Iberoamericana de Protección de Datos, s.f. A e ILDA et al., s.f.). Esto no significa que los demás países no tengan ninguna regulación ni trabajen hacia ella:

» Algunos países como Bolivia ya están trabajando en una regulación en la materia (Delicia Graciela Loayza Martínez, Profesional de Gestión Interinstitucional de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación de Bolivia (AGETIC), "Comunicación Personal", 2023).

El proyecto "Los datos personales y sus leyes" de la Iniciativa Latinoamericana por los Datos abiertos (ILDA), Al Sur y el Banco Interamericano de Desarrollo (BID) revisan el grado de avance de las leyes de datos personales entre los países miembros del BID, contrastándolas con el Estándar Iberoamericano de Protección de Datos a través de 45 indicadores[2]. Según el proyecto, los países con leyes que más se ajustan al Estándar serían Barbados, México y Ecuador, mientras que Chile, Bahamas y Costa Rica tienen las leyes que más difieren de él. La gráfica a continuación muestra el nivel de paralelismo entre las leyes nacionales de varios países de América Latina y el Caribe con el Estándar antes mencionado (ILDA et al., s.f.).



Gráfica 4. Número de coincidencias entre las leyes de protección de datos nacionales en América Latina y el Caribe y el Estándar Iberoamericano de Protección de Datos (ILDA et al., s.f.)

2 Se busca entender qué tanto las leyes de privacidad de diferentes estados coinciden con 45 elementos del Estándar Iberoamericano de Protección de datos: alcance del encargado; condiciones para el consentimiento; consentimiento para el tratamiento de datos personales de niños, niñas y adolescentes; definiciones; derecho a la limitación del tratamiento de datos personales; derecho a la portabilidad de los datos personales; derecho a no ser objeto de decisiones individuales automatizadas; derecho de acceso; derecho de cancelación; derecho de oposición; derecho de rectificación; derechos ARCO; ejercicio de los derechos ARCO y de portabilidad; evaluación de impacto a la protección de datos personales; excepciones generales al derecho a la protección de datos personales; formalización de la prestación de servicios del encargado; mecanismos de autorregulación; naturaleza de las autoridades de control y supervisión; notificación de vulneraciones a la seguridad de los datos personales; objeto; oficial de protección de datos personales; ponderación del derecho a la protección de datos personales; principio de calidad; principio de confidencialidad; principio de finalidad; principio de lealtad; principio de legitimación; principio de licitud; principio de proporcionalidad; principio de responsabilidad; principio de seguridad; principio de transparencia; principios aplicables al tratamiento de datos personales; privacidad por diseño y privacidad por defecto; reconocimiento de medidas proactivas; reglas generales para las transferencias de datos personales; reparación del daño, régimen de reclamaciones y de imposición de sanciones; subcontratación de servicios; tratamiento de datos personales de carácter sensible; tratamiento de datos personales de niños, niñas y adolescentes; ámbito de aplicación objetivo; ámbito de aplicación subjetivo; ámbito de aplicación territorial; establecimiento de mecanismos de cooperación internacional.

De acuerdo con el estudio, los siguientes ejes son los que menos coincidencia tienen con el Estándar en la región: subcontratación de servicios (tan solo 21% de los países de la región coinciden totalmente o parcialmente con los elementos), ponderación del derecho a la protección de datos personales (21%), privacidad desde el diseño y privacidad por defecto (31%), oficial de protección de datos personales (42%), formalización de la prestación de servicios del encargado (42%), derecho a la portabilidad de los datos personales (42%), alcance del encargado (42%), principio de responsabilidad (52%), notificación de vulneraciones a la seguridad de los datos personales (52%), consentimiento para el tratamiento de datos personales de niños, niñas y adolescentes (52%), tratamiento de datos personales de niños, niñas y adolescentes (57%).

Si bien son numerosos los países de la región que cuentan con una ley de privacidad, existen discrepancias en cuanto a su actualización. Por un lado, destaca Brasil que está trabajando en La Ley General de Protección de Datos Personales de Brasil o LGPD (Lei Geral de Proteção de Dados Pessoais, en portugués brasileño), inspirada en el GPDR de la Unión Europea de 2016. Por otro lado, está Argentina que, si bien actualizó su regulación en 2016 para regir la transferencia de datos personales entre fronteras, se considera que se encuentra desactualizada, ya que es posible observar un notable deterioro en su sistema de protección de datos personales. Recientemente, se ha denunciado que el sector público argentino sería el mayor infractor de la Ley de Protección de Datos Personales (Bordachar, 2022).

Como se puede observar, varios países en las regiones de América Latina y el Caribe han implementado leyes de protección de datos personales y otros pendientes de promulgación. Sin embargo, existen diferencias notables en la actualización y eficiencia de cumplimiento de estas leyes por país. La diversidad y complejidad de los contextos resaltan la importancia de seguir monitoreando y adaptando las regulaciones para abordar los desafíos cambiantes en la protección de datos personales en la región.

Ahora bien, existen otros enfoques que se pueden tomar en cuenta para promover el uso responsable de los datos, como lo son las tecnologías que preservan la privacidad, así como los enfoques institucionales que se analizarán en las siguientes secciones.

ENFOQUES TÉCNICOS Y TECNOLÓGICOS

Además de ver el lente desde una perspectiva regulatoria, las diferentes partes interesadas están buscando desarrollar sistemas y métodos técnicos o tecnológicos para promover una mejor privacidad y gobernanza de datos desde el diseño. De las oportunidades que nacieron en el 2018 para promover el uso seguro de datos por varias partes están los fideicomisos de datos, antes de que apareciera la terminología de Tecnologías que Preservan la Privacidad conocidas como PETs, por sus siglas en inglés.

A medida que va evolucionando la innovación tecnológica, el tema de la privacidad se ha vuelto prioritario, sobre todo para armonizar el aprovechamiento de los datos y la privacidad. En muchas jurisdicciones, los principios de Privacidad desde el Diseño (PbD) son obligatorios y las PETs surgen como posibles soluciones para cumplir con ellos. Por lo tanto, las personas responsables del tratamiento de datos deben de anticiparse y tomar medidas técnicas y organizativas para garantizar la incorporación de estos requisitos desde el diseño en sus productos y servicios.

Como consecuencia, se están desarrollando diversas estrategias basadas en técnicas criptográficas y estadísticas innovadoras y cambios estructurales en el procesamiento de datos. Estos enfoques están introduciendo nuevas protecciones de privacidad, gobernanza y seguridad digital en la recopilación y procesamiento de datos. Aunque estas técnicas y tecnologías no son recientes, estas presentan novedades en términos de rendición de cuentas y protección de datos durante su uso. Además, tienen la capacidad de realizar modificaciones mínimas en los datos, permitiendo su procesamiento para usos específicos sin revelar la información que contienen (OCDE, 2023).

A pesar de lo anterior, no existe un consenso en la definición de PETs, ni en su categorización. Una de las razones de la falta de acuerdo en las existentes técnicas y en su nivel de madurez. Sin embargo, se presentan a continuación algunas definiciones:

OCDE (2002)	"Tecnologías que Preservan la Privacidad (PETs) suelen referirse a una amplia gama de tecnologías que ayudan a proteger la privacidad personal. Desde las herramientas que proporcionan anonimato hasta las que permiten al usuario elegir si se revela su información personal, cuándo y en qué circunstancias, el uso de Tecnologías que Preservan la Privacidad ayuda a los usuarios a tomar decisiones informadas sobre la protección de su privacidad".

Agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2015)	"Soluciones de software y hardware, es decir, sistemas que engloban procesos técnicos, métodos o conocimientos para lograr una funcionalidad específica de privacidad o protección de datos o para proteger frente a los riesgos de la privacidad de una persona o un grupo de personas".
Oficina del Comisionado de Información (ICO, 2022) del Reino Unido	"Tecnologías que pueden ayudar a las organizaciones a compartir y utilizar los datos de las personas de forma responsable, legal y segura, entre otras cosas minimizando la cantidad de datos utilizados y cifrando o anonimizando la información personal".

En palabras más sencillas, podemos decir que las PETs preservan la utilidad de los datos al mismo tiempo que minimizan los peligros para la privacidad. Algunas de sus aplicaciones ventajosas son (Simmons+Simmons, 2022):

» Ayudar a demostrar el cumplimiento del principio de minimización de datos y garantizar un nivel adecuado de seguridad en el tratamiento de datos personales.

» Incluir sólidas soluciones de anonimización y seudonimización, así como reducir los riesgos asociados a posibles violaciones de datos personales, haciendo que sean incomprensibles para usuarios no autorizados.

» Permitir el acceso a conjuntos de datos personales que, de otra manera, se consideran demasiado sensibles para compartir.

La siguiente tabla (OCDE, 2023) ofrece un panorama del tema, las diferentes tecnologías, sus aplicaciones y retos y limitantes:

Tipo de PET	Tecnología Clave	Aplicaciones actuales y potenciales *	Retos y limitantes
Herramientas de ofuscación de datos	Anonimización / seudonimización	Almacenamiento seguro	• Asegurarse de que la información no se filtre (riesgo de re-identificación) • Sesgo amplificado sobre todo para datos sintéticos • Falta de capacidades
	Datos sintéticos	Aprendizaje de máquina preservador de la privacidad	
	Privacidad diferencial	Oportunidades de investigación	
	Comprobantes zero-información	Verificar información sin necesidad de divulgación (ej. verificación de edad)	• Las aplicaciones siguen en fases iniciales
Herramientas de procesamiento de datos encriptados	Encripción homomórfica	• Computar datos encriptados en una misma organización • Computar datos privados que son muy sensibles para divulgar • Localización y descubrimiento de contactos	• Retos de limpieza de datos • Impedir filtraciones de información • Costos de computación más altos
	Computación multipartita		
	Ambientes de ejecución confiables	• Computar usando modelos que deben permanecer privados	• Costos de computación más altos • Retos de seguridad digital

Analítica federada y distribuida	Aprendizaje federado	• Aprendizaje de máquina preservador de la privacidad	• Necesidad de conectividad fiable • Se necesita compartir información sobre los modelos de datos con el procesador de datos
	Analítica distribuida		
Herramientas de responsabilidad de datos	Sistemas responsables *(accountable)*	• Establecer y hacer cumplir reglas sobre cuándo se puede acceder a los datos • Rastreo inmutable del acceso a los datos por controladores de datos	• Casos de uso limitados y carecen de aplicaciones independientes • Configuración y complejidad • Riesgos de privacidad y protección de datos en caso de uso de tecnologías de contabilidad distribuida • Retos de seguridad digital • No se consideran PETs en el sentido estricto del término
	Umbral secreto compartido *(threshold secret sharing)*	/	
	Almacenes de datos personales / Sistemas de Manejo de Información Personal	• Proporcionar a los titulares de los datos el control sobre los mismos	

Nota: (*) Sólo se incluye una aplicación por temas de legibilidad.

Tabla 1. Panorama de los PETs principales, sus oportunidades y retos (OCDE, 2023).

La Caja 8 a continuación ofrece definiciones más profundas de varias de las tecnologías mencionadas en la tabla anterior:

Caja 8. Definición de algunas PETs

PET	Definición
Privacidad diferencial (differential privacy)	Estas técnicas introducen pequeñas modificaciones (se agrega ruido) a los datos para ocultar información personal mientras se mantienen los patrones generales. Al utilizar la **Privacidad Diferencial** se brinda cierta protección a las personas a la que se refieren los datos, al agregar ruido que no afecta el análisis general. Sin embargo, hace que los datos sean menos confiables y reveladores para las partes interesadas (OCDE, 2023).
Computación multipartita segura (secure multi-party computation o SMPC en inglés)	La **computación multipartita segura (SMPC)** es un subcampo de la criptografía que permite a los datos ser distribuidos y, al mismo tiempo, mantener la privacidad. El funcionamiento de SMPC se centra en permitir que varias partes, cada una con datos o "entradas" (inputs) privadas realicen cálculos conjuntos sin necesidad de revelar sus entradas privadas. Sin embargo, los protocolos de SMPC actuales son considerablemente más lentos que los sistemas centralizados debido a la latencia en la comunicación encriptada y la complejidad de su implementación (Keyless Technologies, 2020).
Análisis federado y aprendizaje federado	El **aprendizaje federado** parte de un enfoque descentralizado para entrenar los modelos de aprendizaje automático. A diferencia de otros enfoques, no implica compartir datos entre dispositivos cliente y servidores globales. En cambio, los datos brutos de los dispositivos periféricos (edge) se utilizan para entrenar el modelo de manera local, lo que brinda una mayor protección a los datos. Sin embargo, la transmisión de información representa un punto de congestión significativo en las redes federadas (Shastri, 2023).
Entornos de ejecución de confianza	Un **entorno de ejecución de confianza (TEE, por sus siglas en inglés)** es una parte separada del procesador principal de un dispositivo que garantiza la seguridad de los datos. Este entorno, aislado del sistema operativo principal, se encarga de almacenar, procesar y proteger la información en un entorno seguro. Los TEE se separan a través de estructuras y funciones criptográficas y también pueden configurarse para que solo acepte un código previamente autorizado. Sin embargo, las soluciones de **TEE** están sujetas a la confianza en los fabricantes de hardware y otros proveedores de servicios en los que se basan (Bernstein, 2023).

Técnicas de desidentificación	Las **técnicas de desidentificación**, como la asignación de tokens (seudonimización[3]), son procesos de eliminación u ocultación de la información personal identificable (IPI) para reducir los riesgos de que la identidad de las personas se relacione con los datos. Sin embargo, no es posible lograr una anonimización absoluta de los datos, lo que significa que no se puede reducir completamente el riesgo de re-identificación de un sujeto de datos (Banco Mundial, s.f.).
Encriptado homomórfico	El **encriptado homomórfico** consiste en transformar los datos en texto encriptado (utilizando una clave que solo las personas autorizadas poseen) que puede ser analizado y manipulado como si aún estuviera en su forma original. Esta técnica permite llevar a cabo operaciones matemáticas con los datos cifrados sin comprometer la seguridad del cifrado, obteniendo un resultado encriptado. Sin embargo, en contraste con la computación de datos sin encriptar, el **cifrado homomórfico** resulta costoso en términos de recursos computacionales y también tiene un rendimiento menor (Gillis, 2022).
Datos sintéticos	Los **datos sintéticos** son información generada por computadoras para probar y entrenar modelos de IA. La idea principal es generar datos artificiales con propiedades estadísticas similares a una fuente original de datos, sin realmente referirse a ninguna persona, garantizando al mismo tiempo su utilidad para fines específicos. Sin embargo, la reidentificación sigue siendo posible si los registros de los datos de origen están presentes en los datos sintéticos (OCDE, 2023).

A continuación, la Caja 9 profundiza en las aplicaciones actuales de algunas PETs.

Caja 9. Aplicaciones de las PETs

Existe una variedad de aplicaciones de estas tecnologías, particularmente interesantes para aquellos sectores que usan información sensible como el financiero o de salud, entre otros.

Una aplicación interesante es el poder usar datos cifrados, es decir, en formato codificado, para realizar ciertos procesos. Por ejemplo, durante la pandemia, se usó el cifrado homomórfico para poder entrenar un sistema de IA con datos altamente sensibles pero cifrados, lo que permitió avanzar el entendimiento de la enfermedad sin nunca poner en riesgo la privacidad de las personas sujetas de los datos.

Además de incluir técnicas que cifran los datos, las PETs también pueden volver las bases de datos inutilizables, con el fin de que no se pueda re-identificar a individuos con base en la información obtenida en caso de hackeo o filtración de datos. A una de estas técnicas se le llama privacidad diferencial, lo que implica agregar cierta aleatoriedad en los datos de forma que se mantengan los mismos resultados esta-

3 Se trata de eliminar información en los datos que pueda llevar a la identificación de una persona, con el objetivo de reducir el riesgo de identificación del individuo. Sin embargo, existe un riesgo residual de que aún se pueda reconstruir la identidad. Los datos seudonimizados mantienen la capacidad de ser reconstruidos cuando se combinan con información identificable almacenada en otro lugar o con conjuntos de datos externos que contienen información identificable (OCDE, 2023).

dísticos. En Estados Unidos, la Oficina de Censos adoptó esta PET para la publicación de censos poblacionales. Una técnica similar busca usar datos sintéticos, que son datos artificiales, en vez de datos reales ligados a individuos, de igual forma, manteniendo la misma información estadística general.

Con el fin de abordar proyectos complejos, como el entrenamiento de algoritmos avanzados, un reto para las técnicas presentadas anteriormente, se desarrollaron otros enfoques.

Algunas técnicas como la computación multipartita segura divide la base de datos entre distintos servidores en la nube que son capaces de procesar datos conjuntamente pero no tienen interacción entre sí. Este enfoque se vuelve útil, por ejemplo, en casos de autentificación para pagos en línea. El aprendizaje federado es bastante similar a la técnica anterior, ya que permite liberar distintas partes de los datos a diferentes propietarios para entrenar modelos de IA para luego volver a juntar los datos procesados en un solo modelo. Esta técnica facilita la colaboración entre farmacéuticas para avanzar la investigación. Cada entidad participante comparte muestras de datos en una plataforma descentralizada y compartida para que los demás puedan usarlos para entrenar su algoritmo, pero en ningún momento se les da acceso directo a los demás a los datos sensibles.

Otra técnica similar es el uso de entornos de ejecución de confianza, que permite cruzar bases de datos para evitar revelar información sensible que no le corresponde a la persona dueña de una base de datos. Esta se usa en aplicaciones de comunicación como signal, permitiendo a usuarios conectar con personas que ya están en la lista de contactos de su teléfono en la aplicación. La información de los contactos se carga a un servidor central y se encuentran coincidencias entre la base de datos de usuarios de signal y la base de contactos del usuario individual. En ningún momento signal tuvo visibilidad de la información, ya que la información del contacto solo se descifrar en el entorno aislado (Del Pozo, 2023).

A pesar de las ventajas que ofrecen estas tecnologías, varias organizaciones como la Oficina del Comisionado de la Información de Reino Unido (ICO) advierte que las PETs no son una solución definitiva para el cumplimiento de la protección de datos. Se deben de tomar en cuenta otro tipo de medidas adicionales para garantizar el procesamiento legal de los datos personales como por ejemplo autenticación,

cortafuegos, copias de seguridad y antivirus, entre otros. Del mismo modo, se han señalado algunos riesgos asociados con el uso de PETs, como la falta de madurez de algunas de estas técnicas, la falta de experiencia en su uso (lo que puede provocar un uso indebido) y posibles errores en su implementación práctica (Simmons+ simmons, 2022).

La investigación y generación de instrumentos en torno a las PETs, sus aplicaciones y limitaciones, está en auge a nivel mundial:

» Desde el **Reino Unido**, en particular el ICO, se creó una guía para la protección de datos en 2022 para apoyar a las organizaciones en su adopción de PETs. Esto incluye un repositorio público de casos de uso, realizado en colaboración con el Center for Data Ethics and Innovation. La Oficina también está apoyando retos para aprovechar los beneficios de las PETs para abordar retos sociales globales, en conjunto con Estados Unidos. Además, a inicios de 2023, el Alan Turing Institute junto con The Royal Society publicaron un reporte sobre el potencial de las PETs para facilitar la gobernanza de datos.

» En **Estados Unidos**, en marzo de 2023, la Casa Blanca lanzó una Estrategia Nacional para Promover la Analítica y Transferencia de Datos Protegiendo la Privacidad, o PPDSA por sus siglas en inglés. Se desarrolló en colaboración con entes gubernamentales, negocios y la sociedad civil. A su vez, la Comisión de Ciencia, Espacio y Tecnología de la Cámara de Representantes propuso un proyecto de ley bipartidista en 2021 para empoderar a la Fundación Nacional de Ciencias (NSF, por sus siglas en inglés) al Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) a liderar esfuerzos de investigación, desarrollo de fuerza laboral y establecimiento de estándares en cuanto a PETs.

» En **Singapur**, la Autoridad de Desarrollo de Comunicaciones (IMDA, por sus siglas en inglés) lanzó un Sandbox de PETs en 2022, permitiendo a empresas interesadas trabajar con proveedores de confianza de soluciones digitales de PETs para desarrollar casos de uso y pilotos. En particular, el piloto busca conectar casos de uso con una gama de proveedores de soluciones PET, brindar apoyo financiero a empresas para definir e implementar proyectos piloto; y ofrecer apoyo regulatorio para garantizar y minimizar preocupaciones, asegurando que las empresas puedan implementar las PETs, cumpliendo con las regulaciones.

» A **nivel internacional**, la Organización de las Naciones Unidas (ONU) creó el PET Lab para incrementar la adopción internacional de bases de datos públicas, mitigando los riesgos a la privacidad. Con esto, busca facilitar la coordinación y colaboración transfronteriza. Anteriormente, en 2019, lanzó una guía sobre las PETs.

Perspectiva desde América Latina y el Caribe

El último reporte de la OCDE sobre enfoques regulatorios y políticos sobre las PETs (Reimbsbach-Kounatze y Reynolds, 2023) únicamente destaca a dos países latinoamericanos: México y Uruguay.

México: vínculos a PETs en las regulaciones y promoción de su uso/innovación

El reporte menciona instancias en las que se hacen alusiones o se podrían usar PETs para el cumplimiento de la normativa, resumidas a continuación:

» **Requisitos de de-identificación:**

La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) ofrecen una definición de la disociación: "El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este." (Cámara de Diputados del H. Congreso de la Unión, 2010).

» **Requisitos de seguridad de datos:**

- La LFPDPPP indica que "todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de

los datos y el desarrollo tecnológico" (Artículo 19). El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) además publicó en 2015 la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.

- A su vez, la LGPDPPSO (Cámara de Diputados del H. Congreso de la Unión, 2017) define las responsabilidades de los controladores de datos (Artículo 16) y requiere que la parte responsable cumpla con las obligaciones de la ley por defecto (Artículo 30). Sin importar el tipo de sistema en el que se encuentran los datos personales o el tipo de procesamiento que se efectúe, el responsable de los datos debe establecer y mantener medidas de seguridad administrativas, físicas y técnicas para la protección de los datos personales. En particular, estas medidas deben proteger de cualquier daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado y debe garantizar su confidencialidad, integridad y disponibilidad (Artículo 31). Cualquier actividad relacionada con el procesamiento de datos personales debe ser documentada y contenida en un sistema de gestión (Artículo 34).

Por otro lado, el gobierno mexicano ya está creando e impulsando espacios para crear mejores prácticas en privacidad, lo que abre un camino natural para la consideración de las PETs. Por ejemplo, cada año, el INAI promueve la innovación vía el Certamen a la Innovación en Transparencia y el Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales. Actualmente, el Certamen de Innovación en Transparencia 2023 se está llevando a cabo con un enfoque en "herramientas, aplicaciones y plataformas tecnológicas que se encuentren en funcionamiento y que trabajen para el beneficio de la Transparencia en México" (Certamen de Innovación en Transparencia, 2023). En 2022, se llevó a cabo el certamen con un enfoque en "promoción de sistemas, aplicaciones y plataformas tecnológicas que diseminan y generan mejores prácticas para fortalecer el acceso a la información pública, transparencia y responsabilidad en México."

El premio, a su vez, busca "promover, reconocer, impulsar, incentivar, difundir y compartir innovaciones y buenas prácticas desde diferentes disciplinas del conocimiento y la práctica, principalmente

aquellas que desarrollen propuestas creativas y efectivas que permitan hacer más eficiente la protección de datos personales en diferentes ámbitos sociales, laborales y culturales. Ello permitirá fortalecer lazos de cooperación y vinculación con el talento de nuestro país en materia de protección de datos personales, sensibilizando, impulsando y construyendo una cultura de privacidad y prevención entre los responsables y encargados del cuidado y tratamiento de los datos personales de los sectores público y privado en México" (Premio de Innovación PDP, 2023).

Estos espacios podrían contribuir a la exploración y el fortalecimiento del tema de PETs en México.

Uruguay: iniciativa destacada de prototipo de políticas públicas

Esta iniciativa es parte del programa global liderado por Meta: Open Loop, que conecta a los y las responsables de la política pública en temáticas de privacidad y otros aspectos tecnológicos con empresas tecnológicas para desarrollar políticas efectivas basadas en evidencia. A través de esta metodología de gobernanza experimental, se co-crean prototipos de política pública para ser probados en los diferentes enfoques alrededor del uso de la tecnología de forma responsable.

El programa Open Loop Uruguay (2023), liderado por Meta y el Eon Resilience Lab de C Minds, junto con el BID y el BID Lab, con el apoyo de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) y Unidad Reguladora y de Control de Datos Personales (URCDP), generó una propuesta de marco legal y práctico en torno a las PETs, de la mano de varias personas expertas regionales, para los fines de este ejercicio únicamente. Una vez teniendo esta propuesta, se probó a inicios de 2023 con 10 empresas y proyectos de gobierno uruguayos que manejan datos sensibles, con el fin de entender qué tan factible era la identificación de riesgos, selección de estrategia de privacidad desde el diseño e implementación de PETs correspondientes para diferentes organizaciones.

Esta prueba permitió recibir retroalimentación sobre la factibilidad en cuanto a finanzas, mano de obra directa, gastos generales (*overhead*, en inglés), equipamiento e infraestructura, inputs y datos y servicios externos. Estos aprendizajes, resumidos a continuación, contribuyeron así al fortalecimiento de la propuesta de marco para poder

entregar las propuestas de política pública a los reguladores uruguayos como producto de este ejercicio.

Si bien el reporte se publicará más adelante, se comparten a continuación unos aprendizajes clave:

1. Es una temática de interés para todos los sectores e industria, como se vio en el ejercicio Open Loop Uruguay. Tanto proyectos públicos como startups y empresas más establecidas aplicaron recursos para aprender, explorar y probar un prototipo de manual técnico en torno a las PETs durante varios meses, involucrando desde los roles más altos de su organización hasta los equipos técnico y legal, mostrando disposición y motivación del ecosistema por las PETs.
2. Entre los beneficios compartidos por los entes participantes, se destacaron:
    a. lidiar con el crecimiento exponencial de sus bases de datos
    b. identificar nuevos riesgos de privacidad
    c. mejorar nivel de madurez en privacidad, seguridad y gestión de datos
    d. fortalecer el cuidado de las personas titulares de los datos
    e. facilitar el intercambio de datos sin vulnerar la privacidad
    f. mejorar su posición en el mercado local y regional
    g. ofrecer mayor confianza a las personas u organizaciones usuarias finales
    h. operar los principios de privacidad por diseño
    i. fortalecer el cumplimiento regulatorio
    j. normalizar el adherir a estándares más altos en cuanto a privacidad de datos

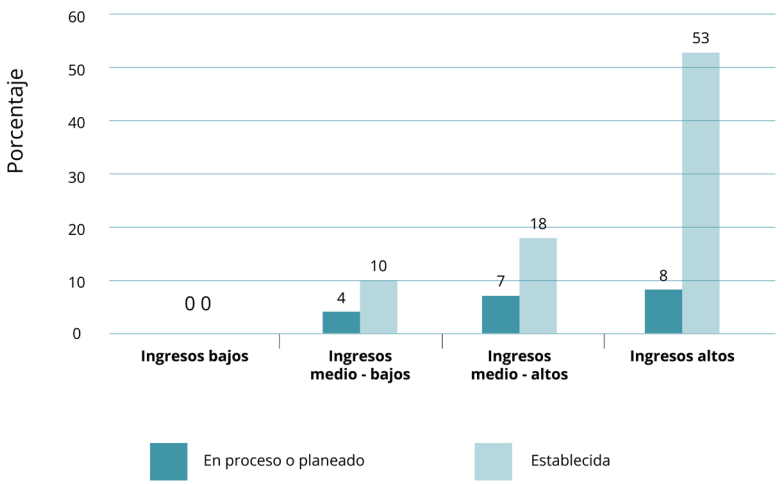
3. Los costos de implementar una o más PET(s) varía considerablemente de un ente a otro, según su tamaño, sector, recursos existentes y enfoque en cuanto a gestión de riesgo de privacidad, por lo que los entes deben de evaluar sus circunstancias únicas para tomar decisiones informadas en cuanto a la asignación de recursos. De los costos más altos identificados para la adopción de PETs se destacaron la capacitación técnica del equipo, la implementación y el mantenimiento. En algunos casos, hasta puede requerir un cambio en la arquitectura de datos.

Con el propósito de promover una mejor privacidad y gobernanza de datos desde el diseño (independientemente de la perspectiva regulatoria) se ha impulsado el desarrollo de sistemas y métodos técnicos como las PETs para reducir los riesgos asociados con posibles violaciones de datos personales. A pesar de los notables avances en investigación y aplicaciones de las PETs en países como Reino Unido, Estados Unidos, Singapur y Uruguay, es esencial destacar que estas herramientas tecnológicas solo son parte de la respuesta a los retos apremiantes de privacidad y gobernanza de datos.

ENFOQUES INSTITUCIONALES

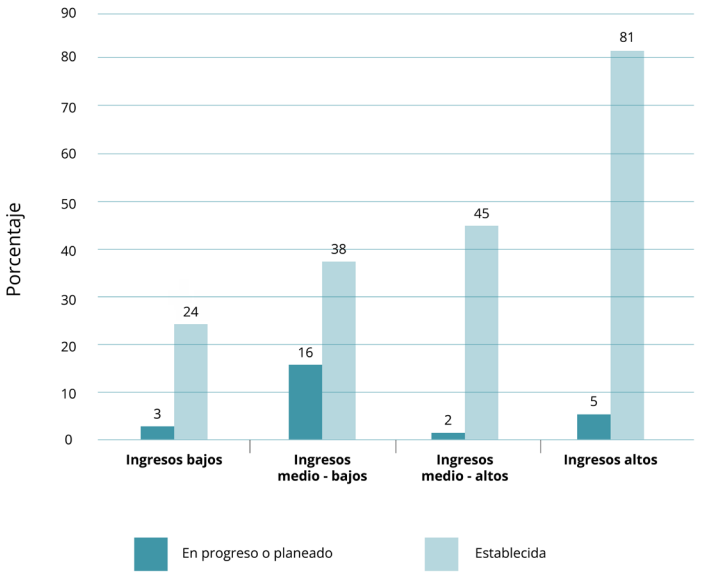
El fortalecimiento de la gobernanza de datos no solo depende de las regulaciones y tecnologías disponibles, sino también de las instituciones públicas existentes para cuidar los datos y maximizar su beneficio. De acuerdo con el Reporte de Desarrollo Global (WDR, por sus siglas en inglés) del Foro Económico Mundial en 2021, tan solo uno de cada cuatro países ya contaba con una entidad de gobernanza de datos mientras que 6% estaba avanzando hacia una o planeaba hacer una (WDR, 2021). La mayoría de estas instituciones se encuentran en países de altos ingresos y, notablemente, ninguno en países de bajos ingresos (por lo general, estos tampoco cuentan con estrategia nacional de datos), como lo demuestra la Gráfica 5.

A su vez, se nota una disparidad en cuanto a la presencia de entidades de protección de datos, las cuales son mucho más frecuentes en países de altos ingresos, como se muestra en la Gráfica 6.



Gráfica 5. Porcentaje de países con una entidad de gobernanza de datos por grupo de ingresos (WDR, 2021 a).

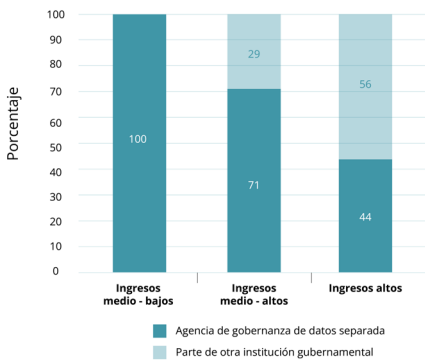
Nota: se consideran 198 economías.



Gráfica 6. Porcentaje de países con una entidad de protección de datos por grupo de ingresos (WDR, 2021 a).

Nota: se consideran 191 economías.

Además, resalta el hecho que cuanto más ingreso tenga la economía, más probable se vuelve que tengan una agencia de datos independiente, y no parte de otra institución gubernamental, como se puede observar en la Gráfica 7.



Gráfica 7. Tipo de entidad de gobierno de datos, por grupo de ingresos por país (WDR, 2021 b).

Una de las posibles razones para ello es que establecer instituciones autónomas puede resultar costoso e ineficiente, ya que demanda recursos adecuados y capacidades técnicas suficientes para funcionar de manera productiva. Sin embargo, la integración de nuevas funciones en las instituciones existentes o la creación de un organismo interinstitucional, como un consejo de gobernanza de datos, puede proporcionar a los gobiernos una mayor flexibilidad en las primeras fases del establecimiento de un marco de gobernanza de datos, respondiendo a la necesidad latente de tener un ente independiente que garantice la neutralidad. Este enfoque también permite a los gobiernos aprovechar el conocimiento de las instituciones pertinentes y, al incorporar más partes interesadas en el proceso, aumentar la inclusividad de la estrategia y el diseño de políticas (WDR, 2021 a).

A su vez, algunas naciones han adoptado una estrategia descentralizada en la que se establece un esfuerzo de colaboración entre ministerios, departamentos y organizaciones para compartir las responsabilidades asociadas a la gobernanza de datos. Por ejemplo, las Oficinas Nacionales de Estadística (ONE) pueden desempeñar un papel central en la elaboración de las Estrategias Nacionales para el Desarrollo de las Estadísticas (ENDE), que forman parte de la estrategia de datos de un país. La eficiencia de la entidad responsable de la planificación estratégica dependerá de su nivel en el gobierno, y, por lo tanto, del nivel de influencia que puede ejercer. Por lo general, se sitúa en el núcleo del gobierno, como el Gabinete del Primer Ministro o el Gabinete del Presidente, en colaboración con la ONE. (WDR, 2021 a).

Perspectiva desde América Latina y el Caribe

En la región, tan solo 45% de los países cuenta con una autoridad de protección de datos independiente o incluida dentro de otra institución gubernamental. Sin embargo, si se omite el Caribe, este número sube a 70%. En particular, destacan ocho países que tienen su propia agencia independiente de protección de datos: Argentina, Brasil, Colombia, Costa Rica, México, Panamá, Perú y Uruguay. En América Latina, solo Belice, Bolivia (que está avanzando en la temática), Nicaragua, Guyana, Surinam y Venezuela no cuentan con autoridad regulatoria en la materia. En el Caribe, tan solo un país tiene autoridad de protección de datos: República Dominicana (Antequera 2023 y Red Iberoamericana de Protección de Datos, s.f. b). Esta información se resume en la Gráfica 12 a continuación.

Gráfica 8. Protección de datos en América Latina y el Caribe (Gráfica realizada por C Minds con base en Antequera, 2023 y Red Iberoamericana de Protección de Datos, s.f. b.).

Ahora bien, en cuanto a gobernanza de datos, existen varios enfoques notables que se resumen a continuación:

» A través de la AGESIC, **Uruguay** ha logrado un marco de gobernanza de datos robusta: incluye la creación de una plataforma de interoperabilidad llamada la Arquitectura Integrada de Gobierno, junto con un marco de arquitectura federada

que propone arquitecturas empresariales para cada una de las agencias del Gobierno (AGESIC, s.f.). Su Agenda de Transformación Digital 2020 demuestra cómo tomar un enfoque desde todo el gobierno y partes interesadas para garantizar que las diferentes capas del ecosistema de gobernanza de datos (plataformas, sistemas, políticas, leyes, estándares e instituciones) se diseñen e implementen de una forma coordinada e inclusiva para llevar a una mejor toma de decisión basada en datos y servicios centrados en el usuario (WDR, 2021 a).

» **Brasil** es uno de los pocos países de ingresos medio-alto con una entidad de gobernanza de datos independiente. Establecido en 2019, el Comité Central de Gobernanza de Datos dirige la transición de Brasil hacia un sector público impulsado por los datos mediante la promoción del intercambio de datos entre los organismos federales y la integración de la información de los ciudadanos en una plataforma única (el Registro Base Ciudadano). El Comité se creó como entidad independiente para garantizar la colaboración y coordinación de alto nivel de las actividades de gobernanza de datos (WDR, 2021 a).

» En **México** destaca la iniciativa de la Red México Abierto, a través de la cual los gobiernos estatales y municipales recolectan y comparten datos en la red de datos abiertos del gobierno central, en línea con los estándares de calidad de datos centralizados (WDR, 2021 a) así como la Plataforma Data México, a través de la cual se permitió la integración, análisis y visualización de datos para mejorar la toma de decisiones de políticas públicas enfocadas en fomentar la innovación, inclusión y diversificación de la economía mexicana (Data México, s.f). El país también cuenta con la Política de Transparencia, Gobierno Abierto y Datos Abiertos de la Administración Pública Federal 2021-2024 cuyo Anexo II establece la Guía de implementación en materia de Datos Abiertos.

La presencia de entidades de gobernanza de datos es escasa a nivel mundial, siendo más notoria en naciones de altos ingresos. Se observa una correlación entre el desarrollo económico y la probabilidad de contar con una agencia de datos independiente. En América Latina, la situación sigue la misma línea, donde menos de la mitad de los paí-

ses disponen de una autoridad de protección de datos, ya sea independiente o integrada en otra institución gubernamental. La limitada representación de estas entidades destaca la necesidad de fortalecer la infraestructura de gobernanza de datos a nivel global y regional.

TENDENCIAS A CONSIDERAR EN ANÁLISIS DE GOBERNANZA Y PRIVACIDAD DE DATOS

Los retos en América Latina para fortalecer la gobernanza y privacidad de datos son numerosos, pero no son únicos de la región. Esta sección explora de forma general cuatro temas o tendencias clave que deben atender las autoridades relevantes de los distintos países que conforman la región al momento de explorar cómo avanzar en la temática. Es importante mencionar que estas tendencias pueden apoyar el fortalecimiento de una estructura organizacional que responda a necesidades de privacidad y gobernanza de datos. Sin embargo, también es crucial tener en cuenta que el cumplimiento y la supervisión son desafíos regionales significativos. Estos aspectos deberían ser prioritarios para los países, ya que consolidarlos es esencial para garantizar el manejo adecuado de la privacidad y los datos en cualquier organización.

Autoridades y regulaciones de protección de datos

Las Autoridades de Protección de Datos, o DPAs, por sus siglas en inglés, es un término principalmente usado en la UE pero que aplica de forma general a las autoridades independientes que supervisan la aplicación de las leyes de protección de datos en un país. En la RGDP de la UE se conocen como Autoridades Nacionales de Supervisión. También están a cargo de asegurarse de que las empresas privadas y entidades públicas cumplan con las leyes de privacidad y en el caso contrario, cuentan con poderes correctivos (Edwards, 2022).

El 55% de la región de América Latina y el Caribe, con la mayoría de los países ubicados en el Caribe, todavía no cuentan con autoridad de protección de datos de ninguna forma. Algunos países como Venezuela ni tienen regulación de protección de datos, ya que solo poseen algunas referencias generales dispersas en normativas (constitución, Ley de los Niños, Ley de la Corte Suprema de Justicia, art. 167), por lo que la privacidad depende de las cláusulas contractuales incluidas por los individuos (Antequera, 2023).

Es crucial que la región de América Latina y Caribe siga promoviendo la existencia de regulaciones de protección de datos personales alineadas con estándares internacionales y la asignación de esta responsabilidad a una institución gubernamental existente o la creación de las autoridades correspondientes.

Ciberseguridad

La ciberseguridad se erige como un componente esencial en la protección de la privacidad y la adecuada gobernanza de datos. Esta última, para ser efectiva, demanda un proceso riguroso que contemple un ciclo de vida de los datos, desde su generación hasta su eventual eliminación o archivado. La ciberseguridad deficiente impacta de manera directa en la gobernanza de datos, pues la integridad de la información puede verse comprometida, en especial si las copias de seguridad están corruptas o si se requiere recuperar información de fuentes no homogéneas. Este panorama compromete la veracidad y autenticidad de los datos, pilares de una adecuada gobernanza. Por otro lado, la privacidad de datos se ve amenazada cuando las medidas de ciberseguridad no son las óptimas, exponiendo información sensible y confidencial a posibles brechas o accesos no autorizados, minando así la confianza de las personas usuarios y partes interesadas involucradas.

En América Latina, la ciberseguridad presenta un desafío considerable, sobre todo, después de la pandemia que conllevó una aceleración a la vida digital y la adopción de trabajo remoto a gran escala. En el primer semestre de 2022, se estima que América Latina sufrió más de 137 mil millones ciberataques, un incremento de 50% en comparación al mismo periodo del año anterior (Fortinet, 2022). El país más afectado habría sido México (con un alarmante 62% de los ataques), seguido de Brasil (23%) y Colombia (4.6%). No solo está aumentando la cantidad de ciberataques, sino también el nivel de peligrosidad, sofisticación y tasa de éxito de las estrategias, como el *ransomware*[4].

Tan solo en 2022, la región sufrió dos ataques masivos: uno en Costa Rica que llevó a un estado de emergencia nacional por paralizar los servicios esenciales del país (Reyes y Kostioukhina, 2023), y en México con el nombrado Guacamaya Leaks, considerado el ciberataque más importante en la historia del país (MIT SMR México, 2023). Ambos casos demuestran la importancia de adelantarse con nuevas regulaciones de ciber resiliencia adecuadas a estos nuevos desafíos. A pesar de esfuerzos reactivos a los ataques de los últimos años, el cerrar las brechas de ciberseguridad en la región requerirá un liderazgo gubernamental revitalizado, pero solo será exitoso a través de un esfuerzo coordinado

4 El ransomware es un tipo de software malicioso que impide el acceso al dispositivo y a los datos almacenados en él, normalmente cifrando los archivos. Un grupo criminal exigirá un rescate a cambio del descifrado. El propio ordenador puede quedar bloqueado, o los datos que contiene pueden ser cifrados, robados o borrados. Los atacantes también pueden amenazar con filtrar los datos que roban (National Cybersecurity Center, s.f.).

con otros actores, y una mayor conciencia cibernética entre las personas formuladoras de políticas, legisladoras, empresas y la sociedad civil.

Interoperabilidad

Actualmente, y en muchos gobiernos de América Latina, la interoperabilidad y la estandarización de los datos siguen siendo limitadas y los datos se siguen gestionando en silos, lo cual obstaculiza el aprovechamiento completo del valor de los datos (Naser, 2021). En efecto, la interoperabilidad entre sistemas se considera un elemento clave para incrementar factores de calidad de datos, ya que permite proveer información vigente, correcta y completa, pero, sobre todo, segura. También juega un rol en el nivel de cooperación posible entre distintos organismos, afectando la cuestión de la gobernanza de datos (Cabello, 2023).

En la región, según Cabello (2023) tan solo algunos países han logrado crear sistemas interoperables dentro de su administración pública, entre ellos:

» Argentina cuenta con INTEROPER.AR23, una herramienta que permite el intercambio de información de manera estandarizada y segura entre los distintos nodos de la Administración Pública Nacional de Argentina. También cuenta con instrumentos para la interoperabilidad de los datos a nivel local, como la guía para la identificación y uso de entidades interoperables del Gobierno de la Ciudad de Buenos Aires.

» En Uruguay, la AGESIC usa un *middleware* integrado por tecnología Microsoft y Java.

» En temas de colaboraciones transfronterizas, cabe mencionar que Argentina, Brasil, Colombia y México están usando la plataforma X-Road (creada por Estonia) para sus abordajes en interoperabilidad. También existe la plataforma RACSEL (Red Americana de Cooperación sobre Salud Electrónica) de LACPass y el BID que reúne a varios países de América Latina y el Caribe, permitiendo el intercambio seguro de datos de salud para responder a problemáticas públicas.

Existen varios elementos que obstaculizan el progreso de los proyectos de interoperabilidad. En algunas ocasiones, se trata el asunto

como si fuera exclusivamente tecnológico, relegándolo únicamente a los equipos de tecnología de la información, quienes no siempre poseen las habilidades o autoridad necesarias para manejarlo. Además, se enfrentan desafíos tecnológicos debido a la presencia de ambientes dispares en aplicaciones y sistemas. A esto se suman los obstáculos derivados de las legislaciones y regulaciones institucionales.

Por otro lado, el sector privado también está explorando cómo generar valor a partir del intercambio de datos seguros. La iniciativa más prominente en este aspecto se lanzó en 2018 en el Reino Unido con la creación del Estándar de Banca Abierta, un marco que busca estandarizar los datos de las grandes entidades financieras para poder compartirlos, con la debida autorización, entre bancos, entidades financieras y consumidores (Beardmore et al., 2018). Estas prácticas, que ya se realizaban previamente, pudieron contar con una capa adicional de seguridad y privacidad al acoplarse con el estándar. De ahí, varios países, entre ellos Australia, están explorando cómo amplificar esta nueva oportunidad a otros sectores como energía y telecomunicaciones, hablando entonces de un Derecho de datos de las personas consumidoras (Gobierno de Australia, 2023). La adopción de estos estándares y marcos promoverán mucha más protección de la privacidad, apoyando un intercambio de datos seguro en la región.

Un marco de gobernanza global

Se debe reconocer que los desafíos planteados por el procesamiento de datos trascienden fronteras nacionales y necesitan esfuerzos coordinados a nivel global. Donde se puede observar un inicio de colaboración internacional relativo a datos es en materia de IA. A continuación, se plasman los avances que han existido en esta materia para plantear un camino que se podría seguir, con espacios dedicados a privacidad y gobernanza de datos. Aquí es importante aclarar que, si bien los espacios creados para fortalecer la colaboración internacional en temas de IA abordan, por la naturaleza misma de esta tecnología, las temáticas de privacidad y gobernanza de datos, también es importante tener conversaciones exclusivamente sobre estos puntos, ya que la privacidad y gobernanza de datos a nivel internacional sigue fragmentada.

En materia de IA, se destacan esfuerzos como las Recomendaciones de Ética de la IA de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y los Lineamientos de IA

de la OCDE, por mencionar algunos. Proyectos como la Alianza Global sobre Inteligencia Artificial (GPAI, por sus siglas en inglés) también han aportado para un entendimiento más profundo del asunto, a través de la generación y propagación de conocimiento. La buena noticia es que estos espacios abordan necesariamente las temáticas de privacidad y gobernanza de datos, por la naturaleza de la IA, pero la mala noticia es que falta impulsar más espacios dedicados exclusivamente a estas temáticas.

Estos documentos han informado las estrategias de IA y/o lineamientos para el uso responsable de más de 70 países a la fecha (Fuentes Nettel, 2023), incluyendo temas de privacidad y gobernanza de datos. Simultáneamente, estas mismas estrategias y lineamientos nacionales han nutrido el debate global en la materia, generando un ciclo virtuoso de aprendizaje y difusión o intercambio de mejores prácticas.

Frente a este desafío, se ha intensificado el interés en crear un espacio internacional para promover la evolución y aplicación ética de tecnologías de procesamiento de datos como la IA. Se dio a conocer que, en noviembre de 2023, el Reino Unido y Estados Unidos encabezaron la inauguración de un Encuentro Mundial sobre IA con la participación de entidades gubernamentales, especialistas, líderes del ámbito empresarial y voceros de la sociedad civil para intercambiar perspectivas sobre la materia. Este evento generó mucha expectativa en el ecosistema de IA, dado el potencial que presenta para una mayor armonización de políticas y marcos regulatorios a nivel global a través de la colaboración multisectorial.

A su vez, la reunión de actores clave en un mismo espacio presentó una oportunidad para facilitar el acceso a fondos para países en desarrollo a través de más programas de cooperación, bancos de desarrollo e iniciativas del sector privado. Estos fondos podrían ir dirigidos a las temáticas desafiantes para América Latina como lo es la instalación de la infraestructura necesaria hasta el fortalecimiento de capacidades, todo orientado hacia los mejores estándares internacionales, así minimizando la fragmentación actual.

Dicho esto, el éxito de esta iniciativa dependerá de muchos factores, entre ellos voluntad política, asignación presupuestaria y liderazgo. De los factores más importantes se destaca la continuidad y la existencia de un mecanismo de rendición de cuentas y transparencia que ocurrirá en paralelo al foro. Sin esto, no se podría dar seguimiento a la implementación de políticas e identificar ajustes necesarios (Fuentes Nettel, 2023).

CONCLUSIÓN

En conclusión, el estado de la gobernanza de datos y la privacidad en el mundo es un panorama complejo y en constante evolución. El rápido avance de la tecnología, unido a la creciente digitalización de la sociedad y sus individuos, ha creado tanto retos como oportunidades a la hora de salvaguardar la información personal y garantizar prácticas de datos responsables.

El contexto mundial ha demostrado que las violaciones de datos y los casos de uso indebido han tenido consecuencias graves y de gran alcance, lo que subraya la urgente necesidad de diseñar e implementar medidas sólidas de protección y gobernanza de datos. La introducción de legislaciones históricas como la RGPD en la UE ha sentado un precedente para las normas de protección de datos en todo el mundo, impulsando iniciativas similares en otros países. El rápido paso de avance de la unión y otras entidades en cuanto a regulación en la materia también ofrece casos de uso y mejores prácticas para inspirar acciones similares y avances constantes en el resto del mundo que, a medida que sucede, ofrece consideraciones, riesgos y oportunidades nuevas a la conversación. Además, la investigación y el desarrollo continuos de tecnologías que mejoren la privacidad, como las PETs, son esenciales para mantener la seguridad de los datos y permitir al mismo tiempo una utilización responsable de los mismos. Si bien estas tecnologías están en etapas iniciales, su inclusión y promoción en varios foros y espacios internacionales resalta la promesa que ofrecen para un futuro en el que el aprovechamiento de los datos no conlleva tantos riesgos de privacidad como lo es actualmente. Para eso, será necesario seguir impulsando ejercicios de gobernanza como los Sandboxes Regulatorios y Prototipos de Política Pública para impulsar su desarrollo responsable.

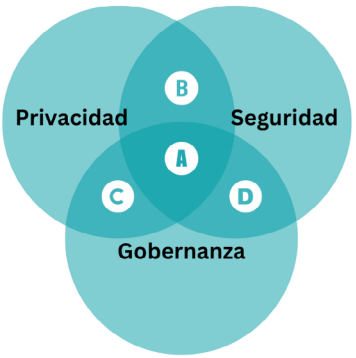
En los últimos años, se han presenciado muchos avances en los distintos países, incluso en la región de América Latina, que permiten impulsar una conversación internacional enriquecedora e informativa para la comunidad global, contribuyendo a la creación de estándares y normas que rijan el desarrollo y actualización de regulaciones nacionales. Será clave para los países de América Latina aprovechar estas oportunidades de aprendizaje e intercambio de conocimientos, dado que los avances en la región aún están por debajo de los adelantos alcanzados en países de alto ingreso. Dicho esto, países como Brasil, Colombia, México y Uruguay, a través de sus respectivas Agencias de Protección de Datos, presentan casos de uso únicos en diferentes aspectos de la temática, posicionándose como líderes en la región.

Sin embargo, a medida que la tecnología sigue avanzando, perseveran retos digitales existentes en la región como la falta o insuficiencia de autoridades o regulaciones de protección de datos, de estrategias de ciberseguridad, de marcos de interoperabilidad de datos y, a nivel más amplio, la inexistencia de un estándar internacional. A estos se suman nuevos desafíos que surgen a medida que avanzan los desarrollos tecnológicos: la adopción generalizada de la IA o el surgimiento de la IA generativa ha aumentado la necesidad de marcos de gobernanza y privacidad de datos cada vez más completos. De cara al futuro, es imperativo fomentar más diálogos mundiales sobre la gobernanza y privacidad de los datos que trasciendan fronteras y culturas. La colaboración entre gobiernos, organizaciones, academia y sociedad civil es crucial para establecer principios comunes, mejores prácticas y normas internacionales que permitan la innovación defiendan las libertades fundamentales y promuevan el progreso de la sociedad.

APÉNDICE

Apéndice 1: Conceptos clave

La privacidad y gobernanza de datos son dos de los tres conceptos que entran en juego para maximizar el valor de los datos, mitigando los riesgos que se pueden presentar para la sociedad. En la Gráfica 9, a continuación, se presentan los tres conceptos con una breve definición (Tech Republic, 2022), destacando sus intersecciones.



A Convergen en la implementación de medidas de seguridad para proteger datos personales y sensibles de accesos no-autorizados, infracciones y usos indebidos.

B Gestión y protección efectiva de datos

C Convergen en procedimientos de gestión de datos: desde políticas de privacidad, gestión de consentimiento, clasificación de datos y evaluaciones de impacto de privacidad.

D Convergen en controles de seguridad, restricciones de acceso y monitoreo de mecanismos para cumplir con políticas de gobernanza y la protección de activos de datos.

Privacidad
La privacidad de los datos, también llamada privacidad de la información, es un aspecto de la protección de datos que aborda el almacenamiento, el acceso, la conservación, la inmutabilidad y la seguridad adecuada de los datos sensibles. También suele asociarse al tratamiento adecuado de datos personales o información de identificación personal, como nombres, direcciones, números de identificación y números de tarjetas de crédito. Sin embargo, la idea también se extiende a otros datos valiosos o confidenciales, incluidos los datos financieros, la propiedad intelectual y la información de salud personal. (Bigelow, 2022)

Seguridad
La seguridad de los datos es la práctica de proteger la información digital contra el acceso no autorizado, la corrupción o el robo a lo largo de todo su ciclo de vida. Es un concepto que abarca todos los aspectos de la seguridad de la información, desde la seguridad física del *hardware* y los dispositivos de almacenamiento, hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye las políticas y procedimientos organizativos. (IBM, s.f.)

Gobernanza
La gobernanza de datos se refiere a diversos acuerdos, incluidas disposiciones técnicas, políticas, normativas o institucionales, que afectan a los datos y a su ciclo (creación, recolección, almacenamiento, uso, protección, acceso, intercambio y eliminación) a través de ámbitos políticos y fronteras organizativas y nacionales. (OCDE, s.f.)

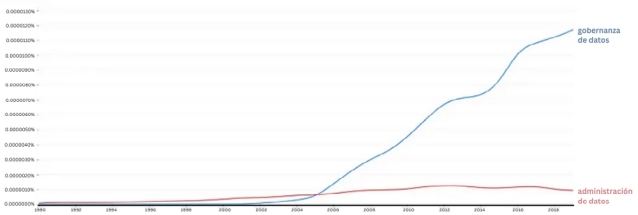
Gráfica 9. Definiciones de términos clave y sus intersecciones (realizada por C Minds).

Si bien cada elemento tiene su propia definición, son conceptos que están en evolución constante, reflejando los cambios en tecnología, sociedad y el avance y conocimiento de personas formuladoras de

política pública. Son trabajos en curso que se experimentan de forma distinta a través de las naciones. A continuación, el reporte se enfocará en las temáticas de privacidad y gobernanza de datos, ofreciendo más contexto sobre cada temática particular.

a. Evolución de la gobernanza de datos

Desde su aparición en los años 60 como función de las tecnologías de la información (TI), el término "gobernanza de datos" ha evolucionado hasta representar uno de los mayores desafíos a los que deben enfrentarse las organizaciones públicas y privadas. El término pasó de ser limitado a los espacios de TI de las organizaciones para volverse tema de conversación general en cuanto se entendió el verdadero potencial que presentaban los datos, marcando el inicio de la transformación digital o la era moderna para la industria (Forbes, 2019). La Gráfica 10 representa las menciones de "gobernanza de datos" (azul) y "gestión de datos" (rojo) en libros y artículos desde 1990, mostrando el creciente interés en la temática.



Gráfica 10. Menciones escritas de "gobierno de datos" (azul) y "administración de datos" (rojo) desde 1990. (Imagen de Atlan, creada con Google Ngrams, traducida por C Minds).

A partir de la primera década de los 2000, el término evolucionó para incluir más elementos como la colaboración, la repartición de la responsabilidad en varios puestos de trabajo y el desmantelamiento de silos de datos. De forma general, se trataba de mejorar las operaciones y funciones dentro de una empresa para promover una estrategia basada en datos. Ese enfoque maximizador del potencial de los datos dio paso a muchas de las empresas exitosas que hoy conocemos.

Sin embargo, la promesa de los datos como generadores de valor "sencillos" (al ofrecer información precisa y accionable) ha presentado retos importantes. Por ejemplo, en el 2018 el *Wall Street Journal*

publicó un artículo hablando de un "ajuste de cuentas mundiales sobre la gobernanza de datos", ya que ese año marcó el inicio de filtraciones masivas de datos que causaron daños reputacionales considerables a varias empresas; entre ellas se destacan Equifax, Facebook, Marriott y Yahoo. El escándalo de Cambridge Analítica, uno de los más conocidos de todos, contribuyó a redefinir el término de gobernanza de datos al hacer notar los riesgos para la sociedad del uso masivo de datos. Esta encrucijada no solo fue el "gran despertar de la privacidad" (Lapowsky, 2019) del público, sino que también destacó la necesidad de políticas públicas que atiendan la vulnerabilidad de los seres humanos frente al uso de datos masivos y sistemas de IA. Para las empresas, significó un nuevo enfoque en disminuir el riesgo de mostrar datos confidenciales a la persona equivocada, de que se utilicen datos erróneos para tomar decisiones y de infringir normativas (Prukalpa, 2021).

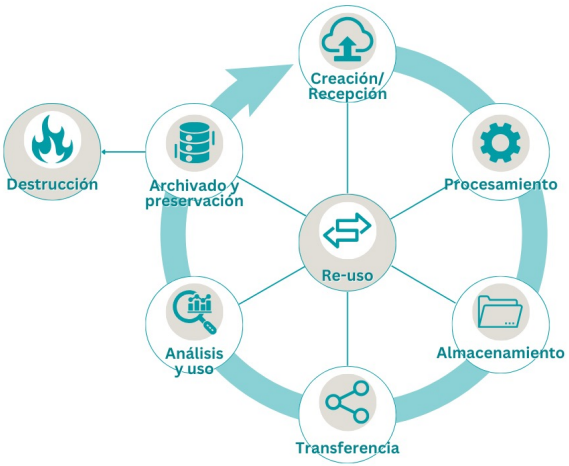
Hoy en día, el tema de "gobernanza de datos" ha evolucionado para cubrir varios aspectos del aprovechamiento responsable de los datos para crear información precisa y accionable para las empresas, pero también para las instituciones públicas, a quienes se les presenta la oportunidad de aprovechar el valor de los datos para mejorar sus operaciones y servicios.

Las iniciativas de gobernanza de datos suelen centrarse en la protección y el riesgo, siguiendo la idea que una mejor gobernanza reducirá el riesgo (Prukalpa, 2021). La ONU lo define como "un enfoque sistémico y multidimensional para crear políticas y reglamentos, establecer el liderazgo para la coordinación institucional y la estrategia nacional, fomentar un ecosistema de datos habilitador y agilizar la gestión de datos" (ONU Departamento de Asuntos Económicos y Sociales, 2020). El Banco Mundial (2021) lo divide en cuatro actividades: 1) planeación estratégica; 2) cumplimiento; 3) generación de reglas e implementación y; 4) aprendizaje y evidencia, tal como se muestra en la Gráfica 11.

Gráfica 11: Gobernanza de datos (Banco Mundial, 2021 a) Traducido por C Minds.

b. Privacidad de datos

Si bien la privacidad ha estado en el centro de las conversaciones a nivel mundial desde hace mucho tiempo, todavía existen algunas dudas sobre qué significa el concepto. Según la Comisión Económica para América Latina y el Caribe (CEPAL) (s.f.) *"El derecho a la privacidad se refiere al estar libre de intrusiones o perturbaciones en la vida privada o en los asuntos personales".* En materia de datos, el término "privacidad" se centra en cómo deben recopilarse, almacenarse, gestionarse y compartirse los datos con terceros, así como en el cumplimiento de las leyes de privacidad aplicables (Data Privacy Manager, 2023). Se debe de considerar la privacidad en todo el ciclo de vida de los datos, el cual es demostrado en la Gráfica 12 a continuación.



Gráfica 12. El ciclo de vida de los datos (Reporte de desarrollo global del Banco Mundial, 2021 b) Traducido por C Minds.

De forma general, se puede pensar en la privacidad de los datos como los derechos de las personas cuyos datos son recolectados, almacenados y procesados (CEPAL, s.f). Estos derechos incluyen el conocimiento de qué datos se retienen y utilizan, así como la posibilidad de corregir cualquier inexactitud.

Incluso las leyes de privacidad no agotan definiciones estrictas de lo que podría definirse como la Privacidad de Datos. Por ejemplo, ni el RGPD en Europa o la CCPA en California ofrecen una definición.

Como se puede observar, la privacidad de los datos no se limita a un solo concepto o enfoque, sino que es una disciplina amplia que abarca normas, prácticas, directrices y herramientas diseñadas para ayudar a las organizaciones a lograr y mantener los niveles adecuados de cumplimiento de la privacidad. La privacidad de los datos suele componerse de seis elementos (Bigelow, 2022):

1. Un marco jurídico que comprende la legislación vigente relacionada con cuestiones de datos, como las leyes de privacidad de datos;
2. Políticas, normas o directrices establecidas en las empresas para proteger la privacidad de los datos de los empleados y empleadas, así como de las personas usuarias;
3. Las mejores prácticas para orientar la infraestructura de TI, así como la privacidad y protección de datos;
4. Terceras partes como cualquier organización externa que interactúen con los datos;
5. La gobernanza de datos implica las normas y prácticas utilizadas para almacenar, proteger, retener y acceder a los datos; y
6. Los requisitos globales se refieren a las diferencias y variaciones en los requisitos de cumplimiento y privacidad de datos entre diferentes jurisdicciones legales en todo el mundo.

La privacidad de los datos brinda el control sobre qué información personal se quiere mantener, además de evitar que su información personal se utilice o comparta sin el consentimiento de la persona sujeta de los datos. También reduce el riesgo de robo de datos u otros delitos informáticos. Por lo tanto, la privacidad ayuda, a que tanto instituciones públicas, empresas como individuos, cumplan con las leyes y normativas de privacidad de datos. Se han promulgado numerosos instrumentos para proteger la privacidad de las personas en el entorno digital y otros (para más información favor de leer la sección de Panorama Global) enfocados en:

» **Prevenir la usurpación de identidad:** A través de la obtención de información personal identificable, como nombre, número de licencia de conducir o número de seguro social, delincuentes pue-

den acceder a créditos, robar reembolsos de impuestos o vaciar cuentas bancarias y causar graves consecuencias.

» **Proteger a las personas consumidoras y/o usuarias de sus servicios:** Hoy más que nunca las personas consumidoras y/o usuarias valoran altamente la privacidad y están preocupadas por cómo se recopilan y utilizan sus datos.

» **Reducir el impacto de los hackeos y las filtraciones de datos:** Sólidas prácticas de privacidad y seguridad de datos pueden actuar como un disuasivo eficaz en ambos casos.

Antes de entrar a detalle en las implicaciones de la naturaleza multifacética de los datos y los diferentes enfoques posibles y complementarios para maximizar su valor mientras se mitigan los riesgos asociados, la siguiente sección ofrece un panorama general del estado de la gobernanza de la IA en el mundo.

BIBLIOGRAFÍA

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (s.f.). *Arquitectura de gobierno y arquitectura empresarial - Arquitectura integrada de gobierno - Arquitectura de gobierno - Liferay.* AGESIC. https://centroderecursos.agesic.gub.uy/web/arquitectura-de-gobierno/arquitectura-integrada-de-gobierno/-/wiki/Arquitectura+de+Gobierno/Arquitectura+de+Gobierno+y+Arquitectura+Empresarial

Antequera, C. (2023). *Data protection in Latin American countries.* Clarke Modet. https://www.clarkemodet.com/en/articles/data-protection-in-latin-american-countries/

Australia Government. (s.f.). *Australia's consumer data right.* https://www.cdr.gov.au/rollout

Azhar, A. (2022). How does data governance affect data security and privacy? *TechRepublic.* https://www.techrepublic.com/article/data-governance-security-and-privacy/

Banco Mundial. (s.f.). *De-identification - Dimewiki.* https://dimewiki.worldbank.org/De-identification#:~:text=De%2Didentification%20is%20the%20process,of%20ethical%20human%20subjects%20research

Banco Mundial. (2021 a). *Governing data.* https://wdr2021.worldbank.org/stories/governing-data/

Banco Mundial. (2021 b). *World Development Report 2021: Data for better lives | Governing Data.* Banco Mundial. https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

Bateman, R. (2023). How the CCPA (CPRA) is similar to the GDPR. *TermsFeed.* https://www.termsfeed.com/blog/ccpa-similar-gdpr/

Beardmore, D, et al. (2018). *What is the potential for open banking in Mexico.* C Minds, Open Data Institute, British Embassy in Mexico. https://www.cminds.co/_files/ugd/de03fd_35feb44c05b5451798cf60a5990cfbb4.pdf

Bernstein, C. (2023). Trusted Execution Environment (TEE). *IT Operations.* https://www.techtarget.com/searchitoperations/definition/trusted-execution-environment-TEE

Bigelow, S. J. (2022). Data privacy (information privacy). *Tech Target.* https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

Bonta, R. (2023). California Consumer Privacy Act (CCPA). State of California Department of Justice. https://oag.ca.gov/privacy/ccpa

Bordachar, M. (2022). *¿Cómo y quiénes cuidan nuestros datos? Legislaciones vigentes en países Latinoamericanos.* Derechos Digitales. https://www.derechosdigitales.org/17759/dia-de-la-proteccion-de-los-datos-personales/

British Council España. (s.f.). *Protección de datos | British Council.* https://www.britishcouncil.es/privacidad-cookies/proteccion-datos#:~:text=La%20ley%20de%20Protecci%C3%B3n%20de%20Datos%20de%20UK%20y%20el,organizaciones%20que%20procesan%20esos%20datos

Burgess, M. (2020). What is GDPR? The Summary guide to GDPR compliance in the UK. *WIRED UK.* https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Cabello, S. (2023). *Análisis de los modelos de gobernanza de datos en el sector público: Una mirada desde Bogotá, Buenos Aires, Ciudad de México y São Paulo.* CEPAL. https://repositorio.cepal.org/server/api/core/bitstreams/9e5b987c-9168-4f88-9503-ca05c6d353ce/content

Cámara de Diputados del H. Congreso de la Unión. *Ley de Protección de Datos Personales en Posesión de los Particulares* [LPDPPP]. 5 de julio de 2010. (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Cámara de Diputados del H. Congreso de la Unión. *Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados* [LPDPPSO]. 26 de enero de 2017. (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Centre for Data Ethics and Innovation. (s.f.). *Repository of Use Cases | PETs Adoption Guide.* https://cdeiuk.github.io/pets-adoption-guide/repository/

Certamen de Innovación en Transparencia 2023. (s.f.). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://certamentransparencia.org.mx/

Comisión Económica para América Latina y el Caribe. (s.f.). *Biblioguías: Gestión de datos de investigación: privacidad de los datos y confidencialidad.* CEPAL. https://biblioguias.cepal.org/c.php?g=495473&p=4398114

Comisión Europea. (s.f. a). *The digital markets act: Ensuring fair and open digital markets.* Comisión Europea. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

Comisión Europea. (s.f. b). *The digital services act: Ensuring a safe and accountable online environment.* Comisión Europea. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Comisión Europea. (2023, 28 junio a). *Data Act: Commission welcomes political agreement on rules for a fair and innovative data economy.* [Comunicado de prensa]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491

Comisión Europea. (2023 b). *Configurar el futuro digital de Europa. Ley Europea de Gobernanza de Datos.* Comisión Europea https://digital-strategy.ec.europa.eu/es/policies/data-governance-act

Comisión Europea. (2023 c). *Proposal for a regulation laying down additional procedural rules relating to the enforcement of GDPR.* Comisión Europea. https://commission.europa.eu/publications/proposal-regulation-laying-down-additional-procedural-rules-relating-enforcement-gdpr_en

Consejo Europeo. (s.f.). *Convention 108 and Protocols.* COE. https://www.coe.int/en/web/data-protection/convention108-and-protocol

Consejo Europeo. (2022, 16 mayo). *El Consejo aprueba la Ley de Gobernanza de Datos.* [Comunicado de prensa]. https://www.consilium.europa.eu/es/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/#:~:text=La%20Ley%20de%20Gobernanza%20de%20Datos%20establece%20garant%C3%ADas%20para%20los,gubernamental%20il%C3%ADcito%20a%20tales%20datos

Consejo Europeo. (2023, 27 noviembre). *Reglamento de Datos: el Consejo adopta nueva legislación sobre el acceso justo a los datos y su utilización.* [Comunicado de prensa]. https://www.consilium.europa.eu/es/press/press-re-

leases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/

Danezis, G., et al. (2015) *Privacy and Data Protection by Design– from policy to engineering.* European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/

Data Guidance. (s.f.). *Jamaica: Data Protection Act enters into force, data controllers granted six-month registration grace period.* Data Guidance. https://www.dataguidance.com/news/jamaica-data-protection-act-enters-force-data

Data México | acerca | Data México. (s.f.). Secretaría de Economía. https://www.economia.gob.mx/datamexico/es/about

Data Privacy Manager. (2023). *5 things you need to know about Data Privacy [Definition & comparison].* Data Privacy Manager. https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

Del Pozo, C. (2023). El papel de las PETs: Nueva era de protección de datos en el impulso tecnológico latinoamericano. *WIRED.* https://es.wired.com/articulos/el-papel-de-las-pets-nueva-era-de-proteccion-de-datos-en-el-impulso-tecnologico-latinoamericano

Edwards, F. (2022). *The purpose of data protection authorities.* Free Privacy Policy. https://www.freeprivacypolicy.com/blog/data-protection-authorities/#:~:text=-Data%20Protection%20Authorities%20supervise%20and,who%20breach%20data%20protection%20laws

Famularo, A. (2019, 11 marzo). *The evolution of data governance.* Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/03/11/the-evolution-of-data-governance/?sh=3cff3e6b5ef7

Fortinet. (2022, 18 agosto). *Fortinet registró 137 mil millones de intentos de ciberataques en América Latina en la primera mitad del año.* [Comunicado de prensa]. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

GDPR Hub. (s.f.). *The history of data protection in Germany.* GDPR Hub. https://gdprhub.eu/Data_Protection_in_Germany

Gillis, A. (2022). *Homomorphic encryption.* TechTarget. https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption#:~:text=Homomorphic%20encryption%20is%20the%20conversion,data%20without%20compromising%20the%20encryption

Greenleaf, G. (2022, 15 marzo). *Now 157 countries: twelve data privacy laws in 2021/22.* 176 Privacy Laws & Business International Report 1, 3-8, UNSW Law Research. https://ssrn.com/abstract=4137418

H.R. 847, *The Promoting Digital Privacy Technologies* Act. (2021, 4 febrero). House Committee on Science Space & Tech - Republicans. https://republicans-science.house.gov/2021/2/hr-847-promoting-digital-privacy-technologies-act

ILDA, et al. (s.f.). *Los datos personales y sus leyes.* Datasketch. https://www.datasketch.co/bid/datos-personales-y-leyes/

INAI. (2015). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Junio 2015.* INAI. https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Infocomm Media Development Authority. (s.f.). *Privacy Enhancing Technologies* (PETS) Sandbox - Infocomm Media Development Authority. https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technologies-sandbox

Information Commissioner's Office. (s. f.). *Privacy-enhancing Technologies* (PETs). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

Information Commissioner's Office. (2022). Chapter 5: Privacy-enhancing technologies (PETs). ICO. https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

Irwin, L. (2022). *The EU Data Governance Act and the GDPR: What you need to know.* IT Governance Blog. https://www.itgovernance.eu/blog/en/the-eu-data-governance-act-and-the-gdpr-what-you-need-to-know#:~:text=Although%20the%20DGA%20isn%27t,way%20their%20information%20is%20accessed

Keyless Technologies. (2021, 13 diciembre). *A beginner's guide to secure multiparty computation.* Medium. https://medium.com/@keylesstech/a-beginners-guide-to-secure-multiparty-computation-dc3fb9365458

Klosowski, T. (2021, 8 septiembre). *The state of consumer data privacy laws in the US (And Why it matters).* New York Times. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lapowsky, I. (2019, 17 marzo). *How Cambridge Analytica sparked the great privacy awakening.* WIRED. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

MIT SMR México. (2023). *Guacamaya Leaks: los 10 secretos que quedaron al descubierto tras el hackeo más grande en México.* MIT Sloan Management Review Mexico. https://mitsloanreview.mx/ciberseguridad/guacamaya-leaks-los-10-secretos-que-quedaron-al-descubierto-tras-el-hackeo-mas-grande-en-mexico/

Naser, A. (2021). *Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación.* CEPAL. https://hdl.handle.net/11362/47018

National Cyber Security Center. (s.f.). *A guide to ransomware.* https://www.ncsc.gov.uk/ransomware/home

National Science and Technology Council. (2023). *National Strategy to advance privacy-preserving data sharing and analytics.* Executive Office of the President of the United States. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

Nettel, P. (2023, 5 julio). *Construyendo un marco de gobernanza global para la IA: ¿Necesitamos un foro mundial?.* Telokwento. https://www.telokwento.com/pj-comexi/construyendo-un-marco-gobernanza-global-la-ia-necesitamos-un-foro-mundial-n21614

Organización para la Cooperación y el Desarrollo Económicos. (2002). *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.* OCDE. https://www.oecd.org/sti/ieconomy/15590267.pdf

Organización para la Cooperación y el Desarrollo Económicos. (2023). *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches.* No. 351, OCDE Publishing, Paris https://doi.org/10.1787/bf121be4-en

Parlamento Europeo. (s.f.). *La protección de los datos personales | Fichas temáticas sobre la Unión Europea* | Parlamento Europeo. https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

Presidencia de la República. (2018, 22 marzo). *Estrategia de Inteligencia Artificial.* MX 2018. [Comunicado de prensa]. https://www.gob.mx/epn/articulos/estrategia-de-inteligencia-artificial-mx-2018

Prukalpa. (2021). *Data governance has a serious branding problem - towards data science.* Medium. https://towardsdatascience.com/data-governance-has-a-serious-branding-problem-7925b909712b

Red Iberoamericana de Protección de Datos. (s.f. a). Legislación. *Red Iberoamericana de Protección de Datos.* https://www.redipd.org/es/legislacion?-nid=183

Red Iberoamericana de Protección de Datos. (s.f. b). *Relación de entidades integrantes de la RIPD.* Red Iberoamericana de Protección de Datos. https://www.redipd.org/es/la-red/entidades-acreditadas

Reyes, I. y Kostioukhina, E. (2023). *Cuatro de los ciberataques más grandes de 2022.* Forbes México. https://www.forbes.com.mx/ad-cuatro-ciberataques-grandes-ciberseguridad-uber-sedena-conti-optus/

Robichaud, F. (2022). *Comparing GDPR to other privacy laws.* Borealis. https://www.boreal-is.com/blog/comparing-gdpr-to-other-privacy-laws/#:~:text=GDPR%20has%20already%20become%20a,shares%20many%20similarities%20with%20GDPR

Rossow, A. (2018). *The birth of GDPR: What is it and what you need to know.* Forbes. https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=1e5d4b7f55e5

Royal Society. (2023). *Privacy Enhancing Technologies* | Royal Society. https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/

Sandvine. (2019). *The Global Internet Phenomena Report.* Sandvine. https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Internet%20Phenomena/Internet%20Phenomena%20Report%20Q32019%2020190910.pdf

Shastri, Y. (2023). *A step-by-step guide to federated learning in computer vision.* V7. https://www.v7labs.com/blog/federated-learning-guide#h1

Secretaría de la Función Pública. (s.f.). *Política de Transparencia, Gobierno Abierto* Datos de la Administración Pública Federal 2021-2024. https://cdn.datos.gob.

mx/apps/guia/Politica_de_Transparencia_Gobierno_Abierto_y_Datos_Abiertos_de_la_APF_2021-2024.pdf

Simmons, D. (2022). *17 countries with GDPR-like data privacy laws.* Comforte Blog https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws

Simmons & Simmons. (s.f.). *ICO publishes draft guidance on privacy enhancing technologies.* Simmons & Simmons https://www.simmons-simmons.com/en/publications/cl94arw416kax0b79ygrxcnvu/ico-publishes-draft-guidance-on-privacy-enhancing-technologies

Stedman, C. y Vaughan, J. (s.f.). *What is data governance and why does it matter?* Tech Target. https://www.techtarget.com/searchdatamanagement/definition/data-governance

Stockburger, P. (2022). *US State Privacy Update: California Privacy Protection Agency announces revised rulemaking timeline under the CPRA.* Privacy and Cybersecurity Law. https://www.privacyandcybersecuritylaw.com/us-state-privacy-update-california-privacy-protection-agency-announces-revised-rulemaking-timeline-under-the-cpra/

Strutt, T., et al. (2023). *Year Three Report: Global Data Governance Mapping Project.* Digital trade and data governance hub. https://globaldatagovernancemapping.org/images/DataGovHub-Year-3/year-three-report.pdf

The Barbados Parliament. (2019). *Data Protection Bill 2019.* https://www.barbadosparliament.com/bills/details/396

The Economic Times. (s.f.). *What is cryptography? Definition of cryptography, cryptography meaning.* The Economic Times. https://economictimes.indiatimes.com/definition/cryptography

U.K.-U.S. *Prize Challenges | Privacy-Enhancing Technologies.* (s. f.). https://petsprizechallenges.com/

UN/DESA *Policy Brief #89: Strengthening data governance for effective use of open data and big data analytics for combating COVID-19* | Department of Economic and Social Affairs. (2020, 21 diciembre). https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-89-strengthening-data-governance-for-effective-use-of-open-data-and-big-data-analytics-for-combating-covid-19/

UNCTAD. (s. f.). *Data protection and privacy legislation worldwide.* UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

United Nations Statistics Division. (s.f.). *UN Guide on privacy-enhancing technologies for official statistics // Task team on privacy enhancing techniques* — UN-CEBD. https://unstats.un.org/bigdata/task-teams/privacy/guide/

Wolford, B. (2023). *What is GDPR, the EU's new data protection law?* GDPR. https://gdpr.eu/what-is-gdpr/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Gobernanza de Datos y las nuevas tecnologías de mejora de la privacidad. Panorama global y retos para Latinoamérica y el Caribe
Primera edición, agosto 2024

Edición a cargo de la **Dirección General de Promoción y Vinculación con la Sociedad**