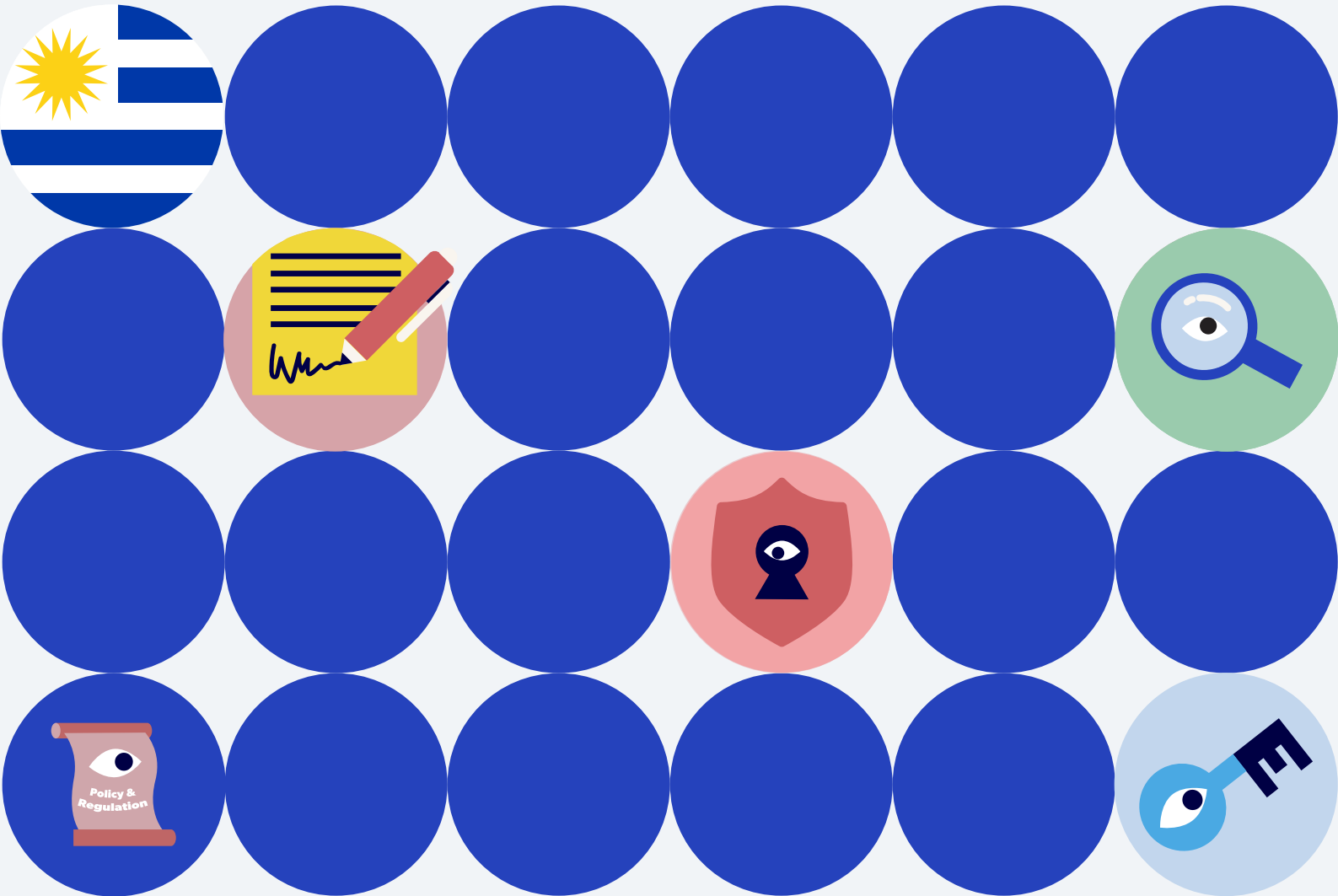
Prototipo de política pública: Guía para la adopción de Tecnologías que Preservan la Privacidad en Uruguay



Index

Prólogo

Los programas Open Loop de Meta en Brasil y Uruguay, que se llevaron a cabo entre 2022 y 2023, marcaron un hito significativo en el avance de las herramientas y metodologías de prototipos de políticas públicas para la gobernanza de tecnologías emergentes en América Latina, en un contexto en el que la idea de experimentación con políticas y entornos regulatorios de prueba (regulatory sandboxes) parecieran haberse convertido en una parte integral de la creación de políticas en los sectores público y privado.

Luego de un exitoso programa sobre transparencia y explicabilidad en México, Open Loop se trasladó al Cono Sur para llevar a cabo un experimento paralelo sobre Tecnologías que Preservan la Privacidad (Privacy Enhancing Techonologies – en adelante "PETs" por sus siglas en inglés) en colaboración con equipos de implementación independientes y varias empresas participantes en Brasil y Uruguay. Esta iniciativa brindó una excelente oportunidad para profundizar en las peculiaridades de cada país, en sus ecosistemas institucionales y de políticas, así como en la naturaleza de los actores que empiezan a implementar PETs en la jurisdicción de cada país. También brindó una oportunidad única para comprender hasta qué punto tienen valor las PETs en la protección de los datos personales de forma general, así como para identificar las similitudes que existen en ambos contextos en términos de retos y oportunidades en torno a la adopción y el uso más amplio de las PETs.

En resumen, Open Loop Brasil y Uruguay generaron tres resultados importantes: primero, los programas contribuyeron a la concientización y al desarrollo de capacidades en torno al tema de las PETs durante la primera etapa del programa; segundo, al trabajar con un consorcio de entidades, personas expertas y formuladores de política pública, el programa originó diálogos e intercambios de conocimientos entre varias partes interesadas de ambos países (incluyendo de forma transfronteriza) que probablemente continúen incluso luego de la conclusión de ese programa; y, por último, la iniciativa colectiva y colaborativa generó evidencia contundente y confiable que sin duda se usará en los procesos de creación de políticas en toda la región y más allá.

A la vez que expresamos nuestra gratitud hacia todas las entidades participantes, observadores, investigadores, y colegas de Meta, que participaron y ayudaron a crear y desarrollar Open Loop Brasil y Uruguay, aprovechamos esta oportunidad para manifestar nuestra confianza en que este informe final representa un primer paso importante y decisivo en la vinculación de la innovación tecnológica y la política, al promover una colaboración estrecha entre quienes crean las tecnologías emergentes y quienes las regulan en América Latina.

Paula Vargas
Directora de Política de Privacidad
e Interacciones para América Latina

Diego Rafael Canabarro
Head of Privacy Policy, Latam

Prólogo

En abril de 2024, las Tecnologías que Preservan la Privacidad (PETs, por sus siglas en inglés) ocuparon el segundo lugar entre las “10 Principales Tecnologías Emergentes para Abordar Desafíos Globales” del Foro Económico Mundial. Este reconocimiento resalta la crucial importancia de salvaguardar la privacidad en una era de rápida transformación digital y evolución acelerada de las tecnologías basadas en datos, incluyendo la Inteligencia Artificial (IA). A medida que el panorama digital sigue expandiéndose, se presentan tanto desafíos como oportunidades para soluciones innovadoras que equilibren el uso de datos con la privacidad personal.

Como organizaciones de la sociedad civil que operan dentro del ámbito tecnológico, tanto el Instituto Liberdade Digital como el Eon Resilience Lab de C Minds (una organización mexicana que explora la intersección entre tecnología emergente, impacto social y ambiental) estamos comprometidos con el desarrollo de estrategias que minimicen los riesgos potenciales de las tecnologías emergentes mientras maximizan su impacto social positivo. Al experimentar con estos temas, podemos redactar recomendaciones de políticas centradas en el ser humano, basadas en nuestros aprendizajes y alineadas con las prácticas y estándares globales.

Dadas las importantes oportunidades que representan las PETs, es fundamental continuar explorando y comprendiendo cómo los mercados en América Latina pueden seguir aprovechando las herramientas de procesamiento de datos mientras se protege la privacidad personal. El programa Open Loop brindó una gran oportunidad porque no sólo estos ejercicios sirven como mecanismos dinámicos para cerrar la brecha entre las discusiones teóricas y las soluciones prácticas, sino también porque aportan diversas perspectivas al involucrar a una amplia gama de partes interesadas, incluidos el gobierno, la academia, la industria y la sociedad civil. Estos esfuerzos colaborativos facilitan la comprensión holística de las sutilezas de las PETs en contextos específicos, asegurando que nuestros hallazgos se traduzcan en recomendaciones integrales y sostenibles

En un contexto global donde se están priorizando las PETs, la publicación de nuestros hallazgos posiciona a América Latina a la vanguardia de las conversaciones internacionales. Esto fortalece la capacidad de la región para sumar perspectivas e innovaciones únicas al diálogo global sobre tecnología y protección de datos. Estos aprendizajes son un paso crucial para asegurar que los beneficios de la transformación digital se realicen de manera amplia y justa, reforzando el papel de la región como líder en el panorama tecnológico global.

Este reporte no solo refleja nuestro compromiso con el despliegue responsable de la tecnología, sino que también es un recurso vital para las personas interesadas que buscan explorar por las complejidades de la IA y la privacidad de los datos. Esperamos que los hallazgos de este informe contribuyan a expandir el conocimiento de la sociedad sobre las PETs, ayuden a las entidades y gobiernos en el proceso de implementación de estas tecnologías, fomenten espacios y discusiones inclusivos y colaborativos, y apoyen a los responsables de políticas en la redacción de marcos adicionales relacionados con la privacidad.

Constanza Gómez-Mont
Presidenta y Fundadora de C Minds

Maria Marinho
Co-fundadora do Instituto
Liberdade Digital

Cláudio Lucena
Universidade Estadual da Paraíba

Prólogo

La Agencia para el Desarrollo del Gobierno Digital y la Sociedad de la Información y del Conocimiento de Uruguay (Agesic) es la entidad líder dentro del Estado en los procesos de transformación digital. Esta transformación viene de la mano de una sólida base jurídica sustentada en normas en materia de acceso a la información pública, ciberseguridad, interoperabilidad, firma e identidad digital, servicios digitales, datos abiertos, accesibilidad, y protección de datos personales, entre otras.

Recientes cambios legislativos dieron un nuevo impulso al rol de la Agencia, posicionándola como líder en el desarrollo e implementación de las Estrategias Nacionales de Datos y de Inteligencia Artificial (IA). Además, se crea la figura de los entornos controlados de prueba o sandboxes regulatorios, como mecanismo para el fomento de la innovación tecnológica segura.

Los datos y el desarrollo de la IA tienen un vínculo inescindible. Las normas de protección de la privacidad deben acompasarse con el uso legítimo de datos para el desarrollo de productos y servicios que redunden en un beneficio de las personas. Y en esto el Estado tiene un rol central, no sólo como usuario y generador de datos en el sector público sino también para proveer herramientas e instrumentos que puedan ser empleados por el sector privado.

El programa Open Loop procuró, a través del acompañamiento a empresas locales de distinta entidad, comprender la problemática en la forma de operativizar tecnologías de mejora de la privacidad o PETs por sus siglas en inglés en el diseño y a dotar de capacidades a estas empresas.

Este programa, acompañado por entidades públicas entre las que se encuentra Agesic, y apoyado por distintas organizaciones y distintos perfiles de colaboradores, logró sus objetivos y propuso una serie de recomendaciones para la adopción de este tipo de tecnologías, necesarias e imprescindibles para una adecuada gobernanza de los datos.

Agesic ha acompañado el programa en el entendido que brinda instrumentos de gran valor para la construcción de las líneas estratégicas que se están desarrollando en materia de datos e IA. Ello por cuanto, comprender las necesidades del sector privado en la adopción de tecnología, es parte instrumental de esta construcción.

Sólo queda agradecer a los impulsores de este programa y a quienes participaron voluntariamente en él. Sus valiosos aportes seguramente servirán para continuar con la discusión en este tema tan relevante para el desarrollo de iniciativas en pro de la innovación y respetuosas de la privacidad de las personas.

Maximiliano Maneiro
Subdirector del Área de Tecnologías de la Información de AGESIC

Información sobre Open Loop

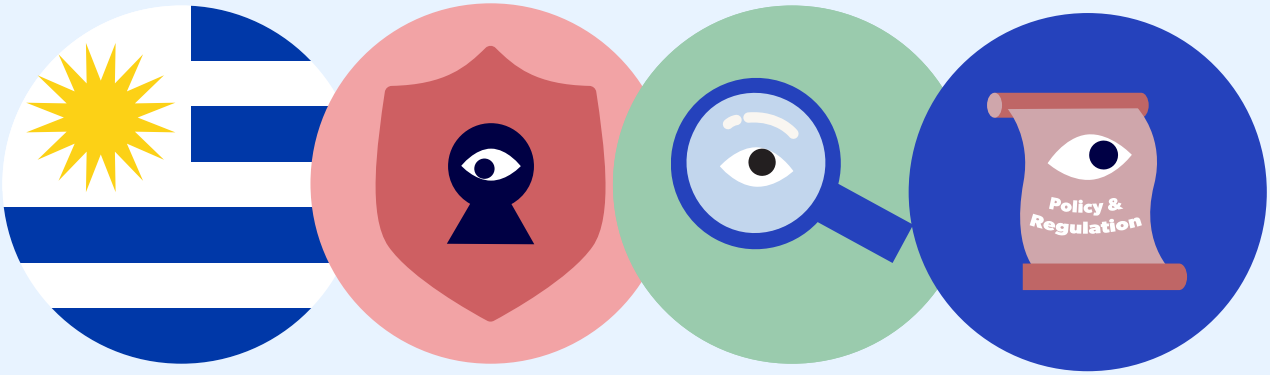
Open Loop de Meta es un programa global que conecta a formuladores de políticas públicas con las empresas de tecnología para colaborar en el desarrollo de políticas públicas efectivas y basadas en evidencia sobre Inteligencia Artificial (IA) y otras tecnologías emergentes.

A través de una metodología estructurada, el grupo de Open Loop crean de forma conjunta "prototipos" de política pública, para probar políticas, regulaciones, leyes o marcos voluntarios sobre IA nuevos o ya existentes. Estas iniciativas multipartitas apoyan los procesos de elaboración de normas y mejoran la calidad de las orientaciones y reglamentos sobre tecnologías emergentes, garantizando que sean comprensibles, eficaces y viables en la práctica.

En este informe, se presentan los resultados y las recomendaciones del programa Open Loop Uruguay sobre PETs, que se inició en septiembre de 2022. Este programa de prototipo de políticas públicas arrancó de forma simultánea con el programa de Brasil, con la intención de guiar y capacitar a las entidades de ambos países para aprovechar y aplicar las PET con el fin de ayudar a reducir la identificabilidad de los datos y mitigar los riesgos relacionados con la privacidad, incluyendo los sistemas de IA. Ambos programas se desarrollaron de forma independiente, y cada uno de ellos contó con un socio local responsable de la implementación del programa. El programa Open Loop Uruguay se llevó a cabo en Uruguay desde septiembre de 2022 hasta abril de 2023 en colaboración con Eon Resilience Lab de C Minds.

Autores: Claudia Del Pozo, Daniela Rojas, David Lehr, Laura Galindo, Maartje Nugteren, Diego Rafael Canabarro y Constanza Gómez-Mont redactaron este reporte.

Cómo citar este reporte
Del Pozo, C., Galindo, L., Rojas Arroyo, D., Lehr, D., Nugteren, M., Canabarro, D. R y Gómez-Mont, C. "Prototipo de política pública: Guía para la adopción de Tecnologías que Preservan la Privacidad en Uruguay" (2024), disponible en https://openloop.org/reports/2024/03/Uruguay_Report_PETs_es.pdf



Agradecimientos

Meta creó el programa Open Loop Uruguay y lo diseñó y ejecutó de forma colaborativa con Eon Resilience Lab de C Minds, el Banco Interamericano de Desarrollo (BID) e IDB Lab, con el respaldo de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) de Uruguay y la Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay.

Queremos agradecer especialmente a las siguientes personas expertas (por orden alfabético) por su valioso tiempo y conocimientos compartidos a lo largo de todo este programa. Sus aportes fueron clave para la implementación de este prototipo de política pública y la creación de este reporte.

- Ana Castillo, Especialista Sénior del BID Lab
- César Buenadicha, Director de la Unidad Discovery del BID
- Gonzalo Sosa, Coordinador de Protección de Datos de URCDP
- Marcelo Cabrol, Director de la División de Escalabilidad, Conocimiento e Impacto del BID Lab
- Marieke Goettsch, Especialista de la División de Competitividad, Tecnología e Innovación del BID
- Matias Bendersky, Representante Nacional del BID en Uruguay
- Maximiliano Maneiro, Subdirector de Tecnologías de la Información de Agesic
- Nancy Ibarra, Asesora del Área Sociedad de la Información
- Nicte Cabañas, ex-líder de comunicaciones y Asistente de proyectos de C Minds
- Norberto Andrade, exdirector de Política de IA de Meta
- Paula Vargas, Directora de Política de Privacidad e Interacciones de Meta
- Virginia Pardo, Directora del área Sociedad de la Información de Agesic

Nos gustaría expresar nuestro agradecimiento y reconocimiento hacia las entidades que colaboraron en el desarrollo de este proyecto:

Ceibal · Codiversity · Digital Sense · Hey Now Bots · Inswitch
República AFAP · Rootstrap · SpaceDev · UTEC · VaFirma

Agradecemos en particular a nuestro grupo de personas expertas, que compartieron sus amplios conocimientos y contribuyeron al desarrollo de la estrategia de investigación del programa: Fernando Vargas, Especialista en privacidad; Javier Barreiro, Vicepresidente de DAMA Uruguay; Lorena Etcheverry, Profesora en la Universidad de la República (Udelar); Matías Jackson, Abogado especializado en regulación y uso de la tecnología; Patricia Díaz, Coordinadora de proyectos e investigadora en Datysoc; Sandra Segredo, Asesora jurídica del rectorado de la Universidad Católica del Uruguay.

También agradecemos a nuestros socios de diseño de Craig Walker Design and Research, en particular, a John-Henry Pajak.

Resumen ejecutivo

Open Loop es un programa global que conecta a las personas formuladoras de políticas con las empresas innovadoras para colaborar en el desarrollo de políticas efectivas y basadas en evidencia en torno a la IA y otras tecnologías emergentes. El principal objetivo de este programa Open Loop fue guiar a entidades de Brasil y Uruguay, para aprovechar, usar y seleccionar PETs con el fin de ayudar a reducir la identificabilidad de los datos y mitigar los riesgos relacionados con la privacidad, incluyendo los sistemas de IA.

Para reducir la brecha entre las expectativas relacionadas con la privacidad y las soluciones tecnológicas, así como para capacitar a los encargados del tratamiento de los datos para procesarlos centrados en la privacidad, se desarrolló y probó un prototipo de política pública en forma de un manual técnico para mejorar los principios de protección de datos mediante las PETs. Este prototipo de política pública tuvo el objetivo de apoyar a las entidades al establecer principios de protección de datos y guiar a las entidades a través de un proceso de tres pasos para hacer operativos principios de privacidad desde el diseño, a la vez que se relaciona con la implementación de PETs.

En este informe, se comparten los resultados de este proceso de creación del prototipo de política pública, que se llevó a cabo en Uruguay desde septiembre de 2022 hasta abril de 2023, en colaboración con Eon Resilience Lab de C Minds e involucró a diez entidades de Uruguay. Estas entidades tienen tamaños diversos y pertenecen a diferentes sectores.

Lo que el programa investigó:

- Hasta qué punto el prototipo de política pública es entendible, viable técnicamente y eficaz en cumplir con los objetivos de política para el público al que va dirigido.
- Nivel de familiaridad y comprensión actual de las entidades participantes respecto de las PETs.
- Brechas y desafíos en la implementación de PETs por organizaciones de Brasil y Uruguay.
- Buenas prácticas y aprendizajes que contribuyen a la implementación exitosa de PETs para ayudar a reducir la identificabilidad de los datos y mitigar los riesgos relacionados con la privacidad.

De acuerdo con los resultados, tanto en Brasil como en Uruguay:

- Las entidades participantes manifestaron una baja familiaridad con las PETs, en especial, con las más avanzadas.
- El manual de PETs ayudó a las entidades a identificar riesgos relacionados con la privacidad y estrategias de mitigación.
- Las entidades participantes enfrentaron limitaciones de costos y recursos humanos.
- La incertidumbre regulatoria es un obstáculo clave para la implementación de las PETs.

Con base en los resultados de los programas Open Loop Brasil y Uruguay, y los comentarios recibidos de las entidades participantes, se ofrecen las siguientes recomendaciones a los organismos reguladores y las personas formuladoras de política pública para la gobernanza de datos, la privacidad y la protección de datos referentes a las PETs:

1. **Las personas formuladoras de políticas públicas podrían adoptar un enfoque flexible y basado en riesgos para el concepto legal de la anonimización.** La medición del nivel de riesgo podría ser una evaluación específica que considere el contexto del procesamiento de datos, las medidas técnicas (PETs) aplicadas a los datos, y las medidas no técnicas (como los controles de acceso y las restricciones legales) que se hayan implementado. Además, la evaluación del riesgo podría centrarse en si las partes que pueden tener acceso realista a los datos, pueden volver a identificar los datos, considerando todas las protecciones aplicadas.

2. **Las personas formuladoras de políticas públicas podrían clarificar que las entidades pueden tratar datos con el fin de reducir el riesgo de identificabilidad.** En particular, en el caso de las jurisdicciones que se basan en leyes similares al RGPD (donde se requiere una base jurídica para el tratamiento de datos), las personas formuladoras de políticas públicas podrían aclarar que: (i) no se necesita una base jurídica para el tratamiento de los datos con el fin de reducir el riesgo de identificabilidad, o (ii) los intereses legítimos, o una base jurídica similar, pueden utilizarse de manera confiable para efectuar dicho tratamiento.

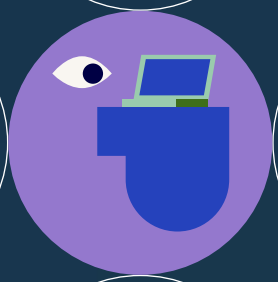
3. **Las personas formuladoras de políticas públicas tienen un rol clave para fomentar el diálogo entre múltiples partes interesadas acerca de las PETs.** Estas conversaciones no solo podrían ayudar a fortalecer la capacidad de las entidades para implementar PETs, sino que también podrían avanzar en el desarrollo de un entendimiento compartido sobre las PETs y su uso eficaz en diferentes casos. Las personas formuladoras de políticas públicas podrían organizar diálogos para explorar estas complejidades, buscando la participación en el proceso de los organismos que establecen los estándares y las asociaciones de la industria.

4. **Las personas formuladoras de políticas públicas podrían invertir directamente en investigación y desarrollo sobre PETs, así como en la educación pública sobre sus beneficios.** Las personas formuladoras de políticas públicas también podrían financiar la investigación y el desarrollo (I+D) de implementaciones de PETs de código abierto, que las pequeñas y medianas entidades podrían usar de forma más sencilla y directa. Además de la I+D, las personas formuladoras de políticas públicas podrían invertir en campañas de educación pública que expliquen a las personas cómo las PETs pueden proteger su privacidad.

5. **Consideraciones adicionales.** Se anima a las personas formuladoras de políticas públicas a que exploren los temas antes mencionados de forma más exhaustiva en entornos de prueba (sandboxes).

Introducción

1



> Al mismo tiempo que han avanzado las tecnologías que analizan grandes cantidades de datos, también lo han hecho aquellas que crean nuevas oportunidades para aumentar la privacidad de las personas. Las Tecnologías que Preservan la Privacidad (PETs) tienen un potencial significativo para hacer frente a muchos riesgos relacionados con la privacidad, al mismo tiempo que permiten los grandes beneficios que el análisis de datos de última generación ofrece a la sociedad en general.

El reconocimiento de estos beneficios ha generado, en los últimos años, un aumento del interés por las PETs, tanto por parte de la industria, como de las personas formuladoras de políticas públicas y defensoras de la privacidad. Sin embargo, a medida que se intensifican los debates en torno a las PETs, es esencial que todas las partes interesadas adquieran un conocimiento profundo de estas tecnologías, los aspectos prácticos de su uso y las formas en que la política pública puede incentivar o desincentivar su implementación.

El programa Open Loop de Meta tuvo como objetivo fomentar esta comprensión a través de iniciativas afines en Brasil y Uruguay, reuniendo a personas expertas, entidades y observadores locales de cada país. Con estas iniciativas, se buscó desarrollar las capacidades de las empresas para implementar PETs y, en el proceso, cuestionarse sobre los desafíos que surgieron y cómo las personas formuladoras de políticas públicas podrían abordarlos.

En este informe, se presentan los resultados y las recomendaciones de política pública claves, obtenidos a partir de las iniciativas de Brasil y Uruguay. El resto de este capítulo introductorio brinda una breve presentación de las PETs, un resumen de la situación normativa mundial relacionado con PETs y describe la metodología en común de las iniciativas de Brasil y Uruguay. El segundo capítulo se centra en aspectos únicos de la iniciativa de Uruguay, incluidos sus participantes y la situación normativa local. El capítulo 3 sintetiza las experiencias de Brasil y Uruguay para extraer una serie de resultados clave. Por último, en el último capítulo, se usan estos resultados para realizar recomendaciones sobre cómo las personas formuladoras de políticas públicas pueden promover la adopción de las PETs.

¿Qué son las PETs?

Las PETs son un conjunto extremadamente diverso de herramientas técnicas que operan de modos muy distintos. En términos generales, las PETs son técnicas criptográficas o estadísticas que preservan el valor informativo de los datos al mismo tiempo que mejoran la privacidad o la seguridad. Sin embargo, dentro de esta definición general, hay muchas técnicas diferentes. A pesar de que no existe un único modo correcto de categorizar las PETs, una posibilidad es agruparlas en cuatro tipos:

PETs que alteran los datos: aquellas, como la seudonimización o la privacidad diferencial, que modifican los datos subyacentes de algún modo.

PETs que alteran la computación: aquellas, como la computación multipartita segura o la análisis federado, que cambian quién calcula una función sobre los datos o cómo lo hacen.

PETs que protegen los datos: aquellas, como el encriptado homomórfico, que cifran los datos o los medios en que se almacenan.

Aprendizaje automático que preserva la privacidad: técnicas, como datos sintéticos o ataques de adversarios, que pueden utilizarse para mejorar o evaluar la protección de la privacidad en el aprendizaje automático y la IA (y a menudo también en otros contextos).

Otra posible categorización de las PETs proviene de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) , que agrupa las PETs en cuatro categorías diferentes: herramientas de ofuscación de datos, herramientas de tratamiento de datos encriptados, análisis federado y distribuido, y herramientas de rendición de cuentas de datos. De nuevo, no existe una forma correcta de categorizar las PETs, pero agruparlas de este modo puede proporcionar un valor heurístico.

Independientemente de cómo se las categorice, hay matices adicionales que dificultan la conversación sobre la implementación de PETs. En primer lugar, las PETs varían enormemente en términos de madurez. Algunas PETs, como los protocolos de encriptado estándar, existen desde hace décadas, mientras que otras, como el encriptado homomórfico y el aprendizaje federado, son mucho más nuevas y aún están en fase de investigación. En segundo lugar, las PETs operan de diversos modos, por lo que proporcionan diferentes grados de protección a la privacidad, además de que algunos son más sencillos de entender que otros. Por ejemplo, es relativamente fácil de entender cómo la eliminación de un identificador directo, como el nombre de alguien, de un conjunto de datos preserva su privacidad, pero otras técnicas, como la computación multipartita segura, mejoran la privacidad de forma más indirecta y menos intuitiva. Por último, a pesar de que las PETs pueden implementarse de forma aislada, en la práctica, suelen combinarse con otras PETs y con herramientas no técnicas que mejoran la privacidad, como lo son los controles de acceso y restricciones contractuales sobre el uso de datos. Las conversaciones técnicas y normativas en torno a las PETs deben reconocer e incorporar estas complejidades.

Global policy landscape

A medida que las PETs han avanzado, también lo ha hecho el interés mundial en ellas. Los gobiernos y las instituciones internacionales manifiestan cada vez más optimismo respecto al papel que las PETs pueden tener en mejorar la privacidad y están dispuestos a aumentar las inversiones en las PETs dentro de sus jurisdicciones. En la tabla 1 a continuación, se presenta un resumen no exhaustivo de las formas en que las personas formuladoras de políticas públicas intentan cumplir estos objetivos. Es importante destacar que, en la tabla 1, no se incluyen ejemplos de Brasil o Uruguay. Las iniciativas correspondientes a Uruguay se describen en el capítulo 2.

Tabla 1: ejemplos de iniciativas y políticas referentes a PETs.

Región/Institución	Iniciativa/Política	Descripción
Estados Unidos 	National Strategy to Advance Privacy-Preserving Data Sharing and Analytics[3]	La Oficina de la Casa Blanca para Políticas de Ciencia y Tecnología definió esta estrategia para aumentar el uso de técnicas similares a las PETs. Entre otras cosas, fomenta la implementación de PETs por parte del gobierno federal, el aumento de las inversiones en investigación y desarrollo, el incremento de la formación sobre PETs, así como una gran colaboración internacional sobre el tema.
Estados Unidos 	Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[4]	Para mejorar la privacidad en la IA, la Orden Ejecutiva exige la formación de una red de coordinación de investigación sobre PETs, así como la identificación de oportunidades para usar PETs por parte de los organismos federales.
Estados Unidos 	National Institute of Standards and Technology (NIST) Guidelines for Evaluating Differential Privacy Guarantees[5]	El NIST elaboró estos estándares sobre la privacidad diferencial para cumplir con el requisito establecido por la Orden Ejecutiva.
Estados Unidos 	Privacy Enhancing Technology Research Act[6]	Este proyecto de ley brinda instrucciones al NIST para financiar investigaciones sobre las PETs, así como a los organismos federales de colaborar en mecanismos de política para promover la implementación de PETs, incluidas estándares y directrices voluntarias.

Reino Unido	Guía preliminar de la Information Commissioner's Office (ICO) sobre la anonimización, la pseudoanonimización y las PETs, y guía definitiva sobre las PETs[7]	Los gobiernos de los Estados Unidos y del Reino Unido se asociaron para financiar el desarrollo de soluciones de PETs para casos de uso específicos.
Reino Unido y Estados Unidos	Retos con premiación (prize challenges) sobre PETs[8]	Los gobiernos de los Estados Unidos y del Reino Unido se asociaron para financiar el desarrollo de soluciones de PETs para casos de uso específicos.
Unión Europea	Revisión de las directrices del Comité Europeo de Protección de Datos (CEPD)	El CEPD indicó en su programa[9] de trabajo 2023-2024 su intención por revisar sus directrices referentes a la anonimización.
Unión Europea	Decisión del Tribunal General de la Unión Europea (UE) sobre la Junta Única de Resolución (JUR) vs Supervisor Europeo de Protección de Datos (SEPD)[10]	Enfatizó que el contexto es importante para determinar si los datos han sido anonimizados y que, al compartir datos, es necesario ponerse en el lugar del receptor para evaluar el riesgo de reidentificación.
Singapore	Entorno regulatorio de prueba de la Personal Data Protection Commission Singapore (PDPC) y la Infocomm Media Development Authority (IMDA)[11]	En este entorno regulatorio de prueba (sandbox), se evaluaron estudios de caso de diferentes empresas, incluida Meta , respondiendo a las preguntas de las empresas sobre la aplicación de las leyes de protección de datos.
Corea del Sur	Directrices revisadas para datos seudonimizados[13]	Estas directrices revisadas abordan el tratamiento de datos seudonimizados, en especial, bajo el contexto de la IA.
Internacional	Informe y talleres sobre las PETs de la OCDE[14]	El informe exhaustivo de la OCDE sobre PETs lo continuarán talleres en los que se explorarán casos de uso y cuestiones políticas.
Internacional	Equipo de trabajo sobre PETs de la Organización de Naciones Unidas (ONU)[15]	Este equipo de trabajo se centra en mejorar el uso de PETs en las oficinas nacionales de estadística.

A pesar de que en la tabla 1 se presenta simplemente un resumen de las iniciativas relacionadas con las PETs alrededor del mundo, la diversidad de iniciativas deja claro que las PETs representan un tema que tiene cada vez más importancia para las diferentes partes interesadas. En particular, los gobiernos expresaron un gran interés en impulsar la implementación de PETs, tanto en el sector público, como en la sociedad y el sector privado de forma general. Otra conclusión es que la relación exacta entre las PETs y las leyes de protección de datos es incierta y está sujeta a una exploración activa por parte de organismos reguladores y tribunales. La mayoría de las leyes de protección de datos no abordan directamente las PETs, es decir, no incluyen disposiciones que hagan referencia específicamente a estas. Dicho esto, la mayoría de las leyes de protección de datos cuentan con principios fundamentales, como la minimización y la seguridad de los datos, y las PETs pueden ayudar a mejorarlos. Además, la mayoría de las leyes excluyen de su ámbito de aplicación los datos que fueron "anonimizados", "desidentificados" o "disociados". Las PETs pueden lograr esto, pero las jurisdicciones están lidiando con cuál es exactamente el estándar para la anonimización. Jurisdicciones como el Reino Unido y Singapur están adoptando un enfoque flexible y basado en riesgos, y la decisión del Tribunal General de la Unión Europea en la JUR pareciera estar impulsando las leyes de la UE hacia esta dirección también. Sin embargo, aún sigue habiendo incertidumbres significativas (incluida una apelación a la decisión de la JUR).

Acerca del prototipo de política pública

Open Loop de Meta desarrolló el **Manual de PETs (el "Manual")**, que serviría como el prototipo de política pública del programa. El Manual es un documento educativo con la finalidad de ayudar a las entidades participantes del programa a entender mejor las PETs, el modo en que pueden disminuir los riesgos de privacidad y la forma que pueden implementarse. Para lograr estos objetivos, en el Manual se definió un proceso de tres pasos que dirigía a las entidades participantes a hacer lo siguiente:

PASO 1

Evaluación de riesgos

Se les recordó a las entidades participantes los principios que guían la protección de datos, se les solicitó que delinearan el ciclo de vida de sus datos y evaluaran los posibles riesgos de privacidad, teniendo en cuenta tanto la probabilidad de un tratamiento de datos no intencional o inesperado, como la magnitud de los daños que podrían resultar de dicho tratamiento.

PASO 2

Identificación de medidas de mitigación de riesgos.

Una vez identificados los riesgos potenciales, se les solicitó a las y los participantes que establecieran qué estrategias podrían implementar para disminuir estos riesgos. Las estrategias potenciales incluían algunas orientadas a los datos (minimización, separación, agregación y ocultar) y otras orientadas a la organización o el tratamiento (informar, controlar, demostrar y hacer cumplir).

PASO 3

Seleccionar las PETs adecuadas

Por último, en el Manual se les solicitaba a las entidades participantes seleccionar y evaluar la aplicación de PETs que respondieran a las medidas de mitigación de riesgos que habían identificado en el paso 2. Las PETs disponibles para la selección incluían técnicas de desidentificación, privacidad diferencial, datos sintéticos, análisis o aprendizaje federado, entornos de ejecución de confianza, computación multipartita segura, técnicas de encriptado y encriptado homomórfico.

Acerca de la prueba

En este programa Open Loop, se llevó a cabo una combinación de métodos para responder preguntas claves en torno a las experiencias con el Manual (consultar el anexo 1 para obtener más detalles). Los hallazgos presentados en este informe se identificaron a través de respuestas a encuestas en línea, talleres secuenciales y temáticos, y entrevistas semiestructuradas con las entidades participantes.

En particular, en la fase de prueba, se pidieron comentarios sobre tres aspectos en particular de cada paso del Manual:

Claridad

Qué tan claramente comunicado y comprensible fue cada paso en el Manual.

Efectividad

Hasta qué punto se logró el objetivo del paso (por ejemplo: hasta: hasta qué punto el paso 3 permitió a las entidades identificar las PETs adecuadas).

Viabilidad

Con qué facilidad, teniendo en cuenta las restricciones operativas y del mundo real, las entidades participantes pudieron llevar a cabo lo prescripto en cada paso.

CAPÍTULO 2

El programa en Uruguay

El programa Open Loop en Uruguay se llevó a cabo con Eon Resilience Lab de C Minds, en colaboración con el Banco Interamericano de Desarrollo (BID) el BID Lab. El apoyo de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) de Uruguay y de la Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay fue fundamental para su éxito. En esta sección, se proporcionan más detalles sobre por qué y cómo se llevó a cabo el programa en Uruguay, incluida la madurez del entorno político de Uruguay para la exploración de estos temas, y las entidades uruguayas que participaron en el programa. Los detalles correspondientes al programa Open Loop de Brasil pueden encontrarse en el **informe de Brasil**.

2

Panorama de la normativa local

Como se describió en el capítulo 1, un desafío de las conversaciones sobre políticas en torno a las PETs es la relación poco clara entre las PETs y las leyes de protección de datos. Las leyes sobre privacidad de datos más integrales no incluyen disposiciones que mencionen de forma explícita a las PETs o indiquen cómo podrían o deberían usarse. En cambio, tales leyes incluyen principios generales sobre la protección de datos, como la minimización de los datos, que las PETs podrían ayudar a lograr, así como exenciones de datos anonimizados, que las PETs podrían ayudar a crear.

La Ley N.° 18331 de Uruguay, Ley de Protección de Datos Personales (LPDP), reglamentada posteriormente por el Decreto N.º 414/009, sigue este enfoque general y usa el término “disociación” en lugar de “anonimización”. El artículo 4 define “disociación de datos” como “es todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.” A pesar de que, normalmente, se debe obtener consentimiento para tratar datos personales, no se requiere consentimiento para los datos disociados. En 2017, la URCDP publicó Criterios de Disociación de Datos Personales para proporcionar más directrices en torno a la disociación. Teniendo en cuenta este interés relativamente reciente en la disociación en Uruguay, esperamos que los aprendizajes del programa Open Loop sean útiles a medida que las conversaciones se sigan desarrollando.

Acerca del grupo

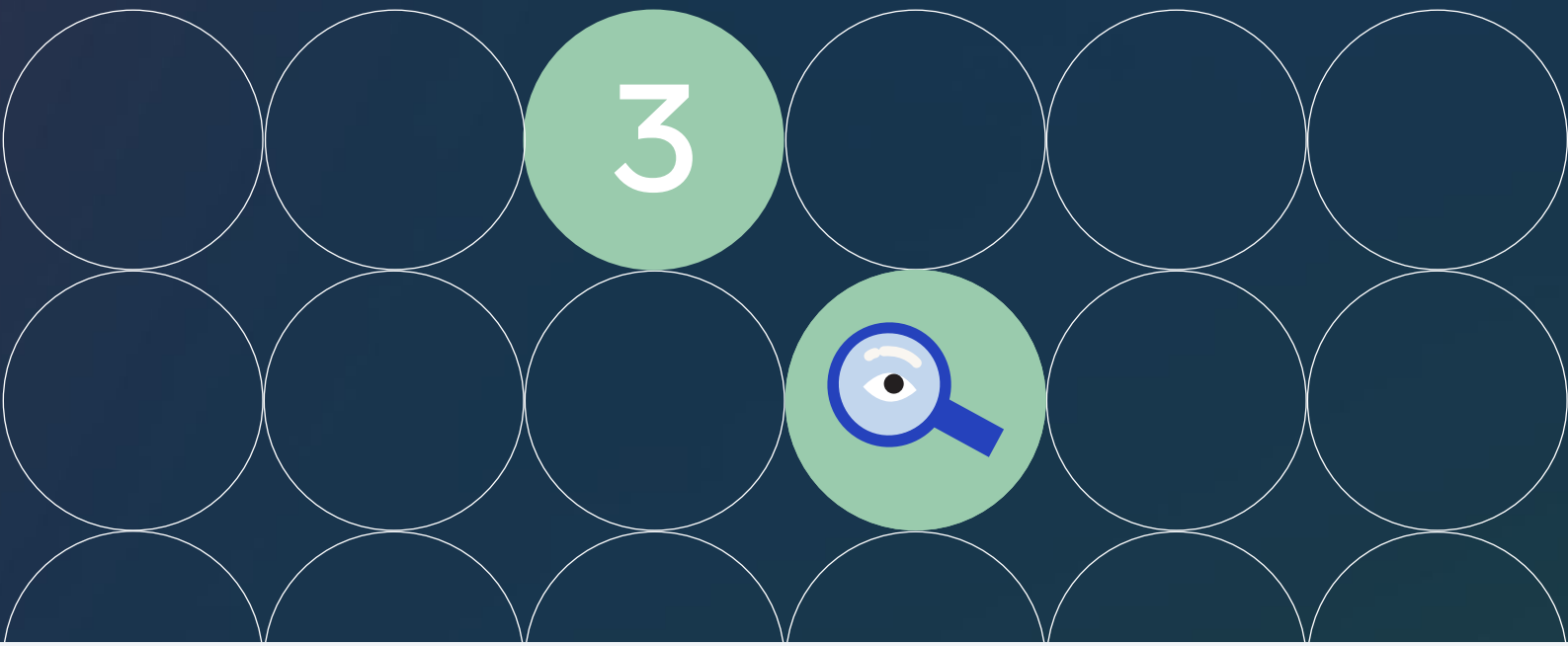
Diez entidades participaron en el programa Open Loop en Uruguay. El grupo de proyectos gubernamentales y empresas fue intencionalmente diverso e incluyó a entidades de diferentes tamaños y de diferentes sectores. En la tabla 2, se presenta más información sobre las entidades.

Nombre	Tipo; sector	Modelo de negocio	Tamaño de la entidad
Ceibal	Proyecto gubernamental; educación	B2C, B2G, B2A	Grande
codiversity	Empresa; HR Tech y Edtech	B2B	Pequeña
Digital Sense	Empresa; tecnología, aprendizaje automático,I+D, y consultoría	B2B	Pequeña
hey now	Empresa; desarrolladores de software	B2B	Pequeña
inswitch	Empresa; Fintech	B2B	Mediana
REPUBLICA AFAP	Empresa; finanzas	B2C	Grande
ROOTSTRAP	Empresa; servicios de TI	B2B	Grande
SPACE	Empresa; servicios de TI	B2C, B2B, B2G, B2A	Mediana
UTEC Universidad Tecnológica	Proyecto gubernamental; educación	B2C	Grande
VaFirma	Empresa; servicios de TI	B2B, B2B2C	Micro

CAPÍTULO 3

Resultados

En los programas Open Loop de Brasil y Uruguay se obtuvieron, en términos generales, resultados similares. Esta sección presenta un resumen de algunos de los resultados más destacados de ambos programas, extrayendo temas generales a partir de las preguntas de investigación relacionadas con la claridad, la efectividad y la viabilidad del Manual. Cuando es el caso, se menciona cualquier diferencia importante observada entre los resultados de ambos países.



RESULTADOS

3.1 Participantes manifestaron una baja familiaridad con las PETs, en especial con las avanzadas

DETALLES

En ambos países, en el inicio de los programas, hubo diferencias en la comprensión de las PETs por parte de las entidades participantes, y su familiaridad con estas. Sin embargo, la naturaleza de estas diferencias fue diferente dependiendo del país. En Uruguay, en el inicio del programa, se les pidió a las entidades que calificaran su familiaridad con las PETs en una escala tipo Likert de cero (falta total de comprensión) a cinco (comprensión total). El promedio de la puntuación fue de 2.5, lo que indica un nivel relativamente bajo de familiaridad con las PETs. Por el contrario, en Brasil, muchas empresas tenían al menos algo de conocimiento sobre las PETs, y casi el 80% de las empresas informaron que ya usaban PETs tradicionales, como las técnicas de anonimización o seudonimización. No obstante, esto fue diferente para las PETs más avanzadas, lo que sugiere un menor conocimiento o comprensión de las PETs más avanzadas.

RESULTADOS

3.2 El Manual de PETs ayudó a las entidades a identificar riesgos relacionados con la privacidad y medidas de mitigación

DETALLES

En términos generales, a las entidades participantes de ambos países el Manual les resultó útil y claro. En Brasil, por ejemplo, dos tercios de las empresas indicaron que el paso 1 del Manual les sirvió para identificar riesgos de privacidad potenciales. Cabe destacar que, probablemente, la principal diferencia entre estas empresas y aquellas a las que el paso 1 del Manual no les resultó útil, fue su tamaño. A todas las pequeñas empresas les sirvió el contenido del Manual, mientras que solo a un poco más de un tercio de las grandes empresas les sirvió. Resultados similares se observaron en Brasil en relación con los pasos 2 y 3 del Manual. La mayoría de las empresas informaron que el paso 2 sirvió de un modo de moderado a significativo para desarrollar su capacidad para identificar estrategias de mitigación relacionadas con la privacidad, y el 75% de las empresas calificaron el material del paso 3 del Manual como algo o extremadamente útil.

En Uruguay, las entidades informaron haber obtenido grandes aprendizajes a partir del Manual. Una entidad afirmó: "Obtuvimos información acerca de los riesgos comunes que podrían surgir en las diferentes etapas del ciclo de vida de los datos". Con respecto al aprendizaje sobre medidas de mitigación del riesgo, otra entidad indicó: "Obtuvimos claridad respecto de ciertas técnicas que actualmente se desestiman o no se consideran". Dicho esto, las entidades de Uruguay informaron que el paso 3 (selección de PETs) fue más difícil de comprender debido a la falta de experiencia con las PETs y el conocimiento actual sobre estas.

RESULTADOS

3.3 Las entidades enfrentaron una gran carga de costos y limitaciones relacionados con recursos humanos

DETALLES

Si bien, en términos generales, a las entidades de Brasil y Uruguay el Manual les resultó útil y sencillo de comprender, estas enfrentaron desafíos significativos en la evaluación de la aplicación de las PETs que seleccionaron en el paso 3. En particular, las entidades de ambos países manifestaron preocupación respecto de que la implementación de las PETs, en particular aquellas más avanzadas, que exigía costos significativos. Estos incluyen costos técnicos, como la inversión en nueva infraestructura de computación y datos, o la modificación de la existente, y costos humanos u operativos, como la contratación y/o capacitación de empleados adicionales.

En Uruguay, se encuestó a las entidades acerca de sus principales preocupaciones respecto de la implementación de PETs (enumerando múltiples preocupaciones). Dos preocupaciones destacaron como las más destacadas, cada una mencionada por seis entidades: “costos de implementación y mantenimiento” y “falta de recursos”. Es notable que únicamente tres entidades contaban con equipos dedicados a la gobernanza de datos, lo cual podría haber contribuido a la regularidad con la que se expresaron estas dos preocupaciones. Estas preocupaciones también impulsaron a que las entidades de Uruguay optaran por la selección de PETs más simples y sencillas de implementar. De las PETs entre las que podían elegir las entidades, dos podrían caracterizarse como relativamente menos complejas y más fáciles de implementar: las técnicas de desidentificación y las técnicas criptográficas. Seis y siete entidades las seleccionaron, respectivamente. De hecho, una entidad afirmó: “La desidentificación podría ser viable en nuestro caso, ya que es válida para cualquier conjunto de datos y el costo de reducir, usar tokens, cifrar o anonimizar es bastante bajo en comparación con otras técnicas más complejas. Lo mismo ocurre con las técnicas criptográficas”. Las únicas otras PETs seleccionadas por algunas entidades fueron privacidad diferencial, datos sintéticos y entornos de ejecución de confianza, cada una de las cuales fue seleccionada sólo por una o dos entidades.

En Brasil, como se mencionó anteriormente, la mayoría de las entidades ya usaban PETs tradicionales, menos complejas, como las técnicas de anonimización y seudonimización. No obstante, las entidades de Brasil enfrentaron desafíos a la hora de implementar las PETs, en especial, aquellas más complejas. Cuando se las encuestó acerca de sus principales preocupaciones en torno a la implementación de PETs, el 75% de las entidades mencionaron los costos de implementación y mantenimiento. En el caso de algunas entidades grandes, las preocupaciones solían girar en torno a los costos de recursos humanos (encontrar equipos de ingeniería disponibles) necesarios para implementar tanto esas técnicas como técnicas más avanzadas. Por ejemplo, una entidad afirmó: “Para aplicar PETs, es necesario tener recursos humanos especializados en la materia, ya que no son fáciles de implementar”.

RESULTADOS

3.4 La incertidumbre regulatoria es un obstáculo clave para la implementación de las PETs

DETALLES

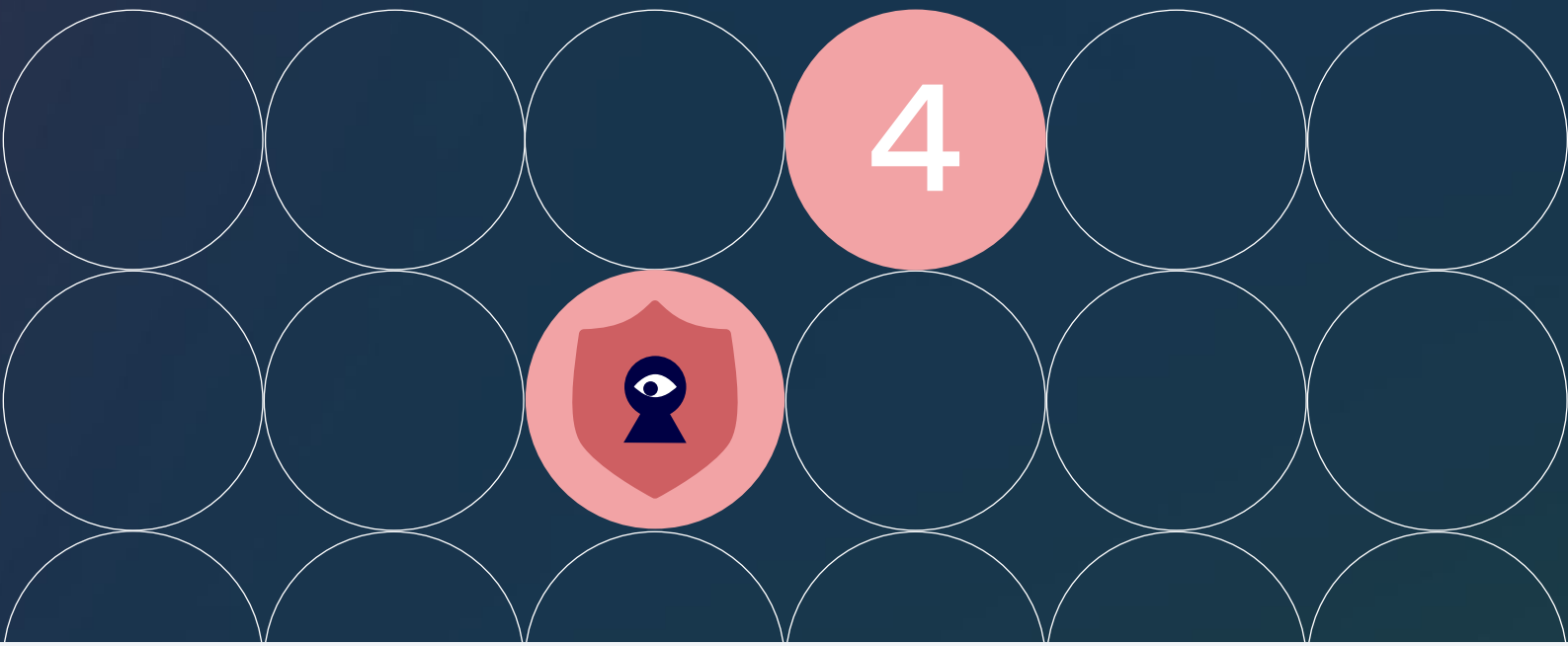
Además de los costos que provienen de la aplicación de las PETs, las entidades de ambos países expresaron el deseo de usar las PETs para mejorar los principios de protección de datos, pero la relación precisa entre las PETs, sin embargo, las leyes de protección de datos no está clara. En Brasil, el 87,5% de las entidades encuestadas citaron la capacidad para cumplir las expectativas regulatorias como un factor para la implementación de las PETs, más que cualquier otro factor. En Uruguay, cuando se encuestó a las entidades acerca de sus principales preocupaciones en torno a la implementación de las PETs, la preocupación que se identificó con mayor frecuencia (fuera de los costos y la falta de recursos) fue los obstáculos regulatorios y legales. Cuatro entidades informaron esto como una preocupación. Esta incertidumbre puede crear en sí misma otro tipo de costo, además de los costos técnicos y operativos: la necesidad de asesoramiento jurídico. De hecho, una entidad de Uruguay mencionó que, además de la infraestructura, sus “principales costos incluyen [...] el asesoramiento jurídico y las posibles modificaciones en la aplicación para cumplir con las políticas de privacidad”.

CAPÍTULO 4

Recomendaciones de política pública

Luego de considerar todos los resultados de los programas Open Loop juntos, las entidades de Brasil y Uruguay están ansiosas por implementar las PETs y observar su capacidad potencial para mejorar los principios de protección de datos. No obstante, varios obstáculos se interponen en su camino. Muchas entidades, en especial, las pequeñas y medianas, no están familiarizadas con las PETs, ni con el conocimiento técnico necesario para implementarlas. Además, la implementación de las PETs, en especial, las más recientes y técnicamente más complejas, implica grandes costos e incertidumbres. Las PETs suelen requerir inversiones financieras significativas sobre nuevas infraestructuras de datos y de capacidad computacional, así como personal con habilidades técnicas pertinentes. Más allá de estos costos, las entidades también enfrentan una gran incertidumbre sobre cómo el uso de las PETs se relaciona con diferentes disposiciones de las leyes de protección de datos, lo que desincentiva las inversiones costosas en las PETs.

Estos desafíos presentan una oportunidad ideal para las personas formuladoras de políticas públicas. Las personas formuladoras de políticas públicas, como las entidades, reconocen cada vez más el valor de las PETs y están buscando incentivar su uso. Los resultados de los programas Open Loop proporcionan una guía al respecto al identificar las causas básicas de los desafíos e incertidumbres de las entidades participantes (causas que las personas formuladoras de políticas públicas podrían tratar de abordar). En esta sección, se proporcionan recomendaciones concretas y aplicables, que esperamos que sean útiles para lograrlo.



RECOMENDACIÓN

4.1 Certidumbre regulatoria e incentivos para la implementación de PETs

DETALLES

Las personas formuladoras de políticas públicas de todo el mundo tienen la capacidad para elaborar o modificar las leyes, regulaciones o interpretaciones, para abordar la incertidumbre regulatoria mencionada por las entidades participantes. En particular, se anima a las personas formuladoras de políticas públicas a:

Adoptar un enfoque flexible y basado en riesgos para abordar el concepto legal de la anonimización.

Para muchas entidades, saber que los organismos reguladores podrían considerar el uso de las PETs como una forma legal de anonimizar los datos es un incentivo contundente. Si los datos se anonimizan a través del uso de PETs, las entidades pueden hacer más cosas con esos datos. No obstante, como se mencionó con anterioridad, el modo en que las diferentes jurisdicciones abordan el concepto legal de la anonimización no está claro. Algunas entidades, como la ICO del Reino Unido, la PDPC, y la IMDA de Singapur adoptaron lo que podría considerarse un enfoque flexible y basado en riesgos. Este enfoque reconoce que la anonimización no tiene que significar necesariamente una reducción del riesgo de identificabilidad a casi cero, ya que podría haber un riesgo residual, aunque sea pequeño. La medición del nivel de riesgo podría ser una evaluación específica de los hechos que considere el contexto del tratamiento de datos, las medidas técnicas (como las PETs) aplicadas a los datos y las medidas no técnicas (como controles de acceso y restricciones legales) que se hayan implementado. Asimismo, como el Tribunal General de la UE indicó en la JUR, la medición del riesgo podría centrarse en si las partes que pueden tener acceso de forma realista a los datos pueden volver a identificar los datos, considerando todas las protecciones aplicadas, y no si cualquier supuesto tercero con recursos y acceso ilimitados a otros datos, podría hacerlo. Se anima a las personas formuladoras de políticas públicas a seguir los pasos de la ICO del Reino Unido, la PDPC y la IMDA de Singapur y el Tribunal General de la UE.

Aclarar que las entidades pueden tratar datos con el fin de reducir el riesgo de identificabilidad.

Además de la incertidumbre sobre cuándo y cómo el uso de PETs puede anonimizar legalmente los datos, las entidades también tienen incertidumbre respecto de si, en primera instancia, el uso de las PETs se considera un tratamiento justificado de los datos personales. A pesar de que hacerlo se alinea claramente con el objetivo de las leyes de protección de datos (aumentar la privacidad de las personas), muchas leyes no indican que este tipo de tratamiento está permitido. Se anima a las personas formuladoras de política pública a abordar esta deficiencia.

En particular, en el caso de las jurisdicciones que se basan en leyes similares al RGPD (donde se requiere una base jurídica para el tratamiento de datos), las personas formuladoras de políticas públicas deben aclarar que: (i) no se necesita una base jurídica para el tratamiento de los datos con el fin de reducir el riesgo de identificabilidad, o (ii) los intereses legítimos, o una base jurídica similar, pueden utilizarse de manera confiable para efectuar dicho tratamiento.

Para estos fines, también se anima a las personas formuladoras de política pública a que exploren estos temas de forma más exhaustiva a través de entornos regulatorios de prueba (sandbox). Los entornos regulatorios de prueba (sandbox) pueden proporcionar oportunidades fundamentales para que tanto las personas formuladoras de política pública como las entidades aprendan en conjunto, en especial, en situaciones (como el uso de PETs) que son técnicamente complejos y nuevos.

RECOMENDACIÓN

4.2 Diálogos entre múltiples partes interesadas en torno a las mejores prácticas y estándares

DETALLES

Cumplen un papel clave a la hora de fomentar el diálogo acerca de las PETs entre múltiples partes interesadas. A las entidades participantes de los programas Open Loop les resultó muy valioso poder aprender de expertos en materia técnica y normativa acerca de las PETs, y las personas formuladoras de políticas públicas de todo el mundo podrían fomentar conversaciones similares en sus propias jurisdicciones.

Estas conversaciones podrían ayudar a consolidar la capacidad de las entidades para implementar PETs, así como favorecer el desarrollo de un conocimiento compartido y cómo estas pueden usarse de forma eficaz en diferentes casos de uso. Como se mencionó anteriormente, las PETs son un grupo diverso de técnicas que operan de diferente forma y proporcionan diferentes niveles de protección a la privacidad. Esto significa que lo que podría considerarse como una práctica recomendada o un estándar para el uso de una PETs dependerá en gran medida de cuál es la PETs y del contexto en el que se implementa. Las personas formuladoras de políticas públicas podrían organizar diálogos para explorar estas complejidades, buscando la participación en el proceso de los organismos que establecen los estándares y las asociaciones de la industria.

RECOMENDACIÓN

4.3 Inversión directa en investigación y desarrollo (I+D), y educación

DETALLES

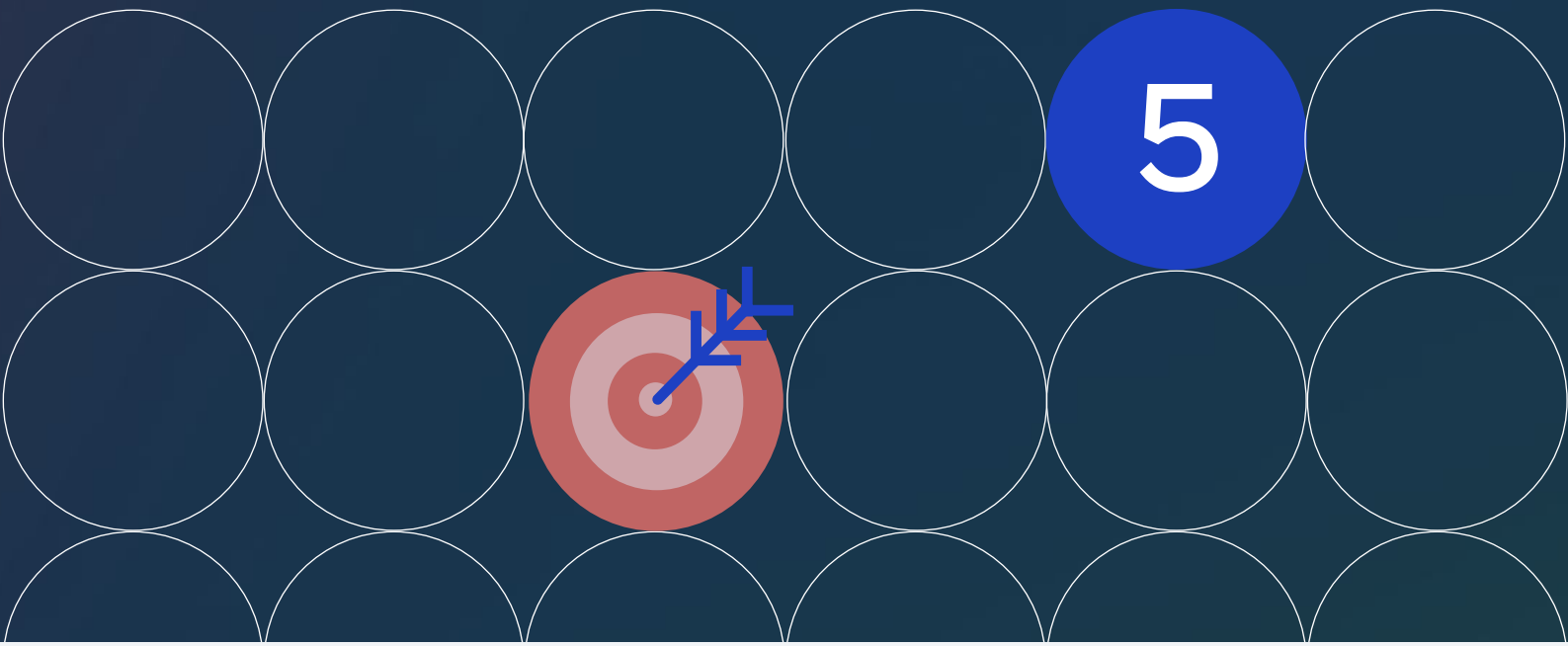
Por último, se anima a las personas formuladoras de políticas públicas a invertir directamente en la investigación y el desarrollo de las PETs, así como en la formación pública acerca de las ventajas de estas. Los resultados de los programas Open Loop demostraron que muchas entidades, en especial, las pequeñas y medianas, simplemente no tenían los recursos y fondos necesarios para implementar las PETs a gran escala. Esta dificultad podría abordarse a través de el financiamiento directo gubernamental en I+D, como hicieron los Gobiernos de Estados Unidos y el Reino Unido con sus retos con premiación (prize challenges), al proporcionar incentivos directos a las entidades para desarrollar e implementar PETs. Las personas formuladoras de políticas públicas también podrían financiar la I+D de implementaciones de PETs de código abierto, las cuales podrían ser utilizadas más fácilmente por pequeñas y medianas entidades directamente disponibles para su uso.

Además de la I+D, las personas formuladoras de política pública podrían invertir en campañas de educación pública que permitieran explicarles a las personas de qué modo las PETs pueden proteger su privacidad. Algunas entidades podrían optar por no implementar PETs si consideran que sus clientes o personas usuarias no entenderán los beneficios de hacerlo, especialmente cuando implementar PETs requiere muchos recursos. Sin embargo, una mayor concienciación pública sobre las PETs podría abordar estas dudas al aumentar la probabilidad de que las personas aprecien las inversiones que las entidades hacen en estas tecnologías.

CAPÍTULO 5

Conclusión y próximos pasos

En resumen, los programas Open Loop en Brasil y Uruguay fomentaron una mayor comprensión de las PETs y cómo aplicarlas entre las entidades participantes. Las sesiones de desarrollo de capacidades y el Manual se percibieron como útiles, pero las entidades participantes se enfrentaron a desafíos a la hora de evaluar la aplicación de las PETs. Muchos consideraron el proceso de implementación de las PETs técnicamente complicado y costoso. Y, a pesar de que las entidades expresar un mayor deseo por usar PETs para mejorar los principios de protección de datos, no estaba claro el modo exacto en que las PETs se relacionan con las leyes de protección de datos, y obtener asesoramiento jurídico al respecto es un costo adicional por considerar. Estos aprendizajes deberían resultarles valiosos a las personas formuladoras de políticas públicas, ayudándoles a elaborar regulaciones y programas que aumenten la certeza regulatoria, fomenten el diálogo entre múltiples partes interesadas y estimulen la investigación y el desarrollo en torno a estas tecnologías prometedoras.



Anexo 1 - Metodología

Alcance

Los programas Open Loop de Brasil y Uruguay se guiaron por las siguientes preguntas generales de investigación:

- **PI1:** ¿En qué medida el prototipo de política pública equilibra la claridad, la viabilidad técnica y la eficacia de la política para el público al que va dirigido?
- **PI2:** ¿Cuál es el nivel de familiaridad y comprensión actual de las entidades participantes sobre las PETs?
- **PI3:** ¿Cuáles son las brechas y desafíos que se les presentan actualmente a las entidades participantes en la implementación de PETs?
- **PI4:** ¿Qué buenas prácticas y aprendizajes pueden contribuir a la implementación exitosa de PETs para ayudar a reducir la identificabilidad de los datos y mitigar los riesgos relacionados con la privacidad?

Se empleó una metodología de investigación combinando métodos cualitativos y cuantitativos. Recopilamos datos de orígenes diversos: investigación documental, entrevistas, encuestas y talleres. Este enfoque de combinación de métodos nos permitió triangular los datos y abordar las preguntas de investigación desde varias perspectivas (consultar la tabla a continuación).

Limitaciones y consideraciones:

El enfoque de combinación de métodos propuesto para este estudio es idóneo para abordar las preguntas y los objetivos de investigación. No obstante, las limitaciones propias de la metodología deben de tenerse muy en cuenta al momento de interpretar los resultados de este informe.

- **Datos informados por las partes interesadas:** el uso de información aportada por las partes interesadas implica un posible sesgo, que requiere precaución en la interpretación.
- **Limitación del tamaño de la muestra:** si bien hubo representantes de diversos sectores, el tamaño de la muestra podría no incorporar todos los matices sectoriales o prácticas emergentes.
- **Alcance temporal:** la investigación capturó un momento temporal específico (desde noviembre de 2022 hasta julio de 2023), y las prácticas pueden evolucionar con el tiempo.

Estas limitaciones exigen una interpretación cuidadosa de los resultados. La triangulación de datos a partir de múltiples fuentes y métodos podría mitigar posibles sesgos. A pesar de que no se puede generalizar a toda la población, la investigación proporciona información y tendencias valiosas dentro de las entidades participantes. En investigaciones futuras, se podrá ampliar el alcance y abordar las prácticas emergentes.

Referencias

[1] Del Pozo, C., Nuno Gomes de Andrade, N., & Rojas Arroyo, D. “Prototipo de Políticas Públicas sobre Transparencia y Explicabilidad de Sistemas de Inteligencia Artificial [Public Policy Prototype on the Transparency and Explainability of Artificial Intelligence Systems] (2023), at: https://openloop.org/ reports/2023/10/Public-Policy-Prototype-on-the-Transparencyand-Explainability-of-Artificial-Intelligence- Systems.pdf

[2] OECD (2023). "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en.

[3] National Science and Technology Council (2023). National Strategy to advance privacy-preserving data sharing and analytics, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

[4] The White House (2023, October 30). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[5] Near, J., Darais, D., Lefkovitz, N., & Howarth, G. (2023, December 11). Guidelines for Evaluating Differential Privacy Guarantees. https://csrc.nist.gov/pubs/sp/800/226/ipd

[6] Privacy Enhancing Technology Research Act, no. 4755, Science, Space, and Technology (2023). https://www.congress.gov/bill/118th-congress/house-bill/4755

[7] Information Commissioner's Office (2023, June 19). Privacy-enhancing technologies (PETs). Information Commissioner’s Office. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

[8] U.K.-U.S. prize challenges | Privacy-Enhancing Technologies. (n.d.). Petsprizechallenges.com. Retrieved May 2, 2024, from https://petsprizechallenges.com/

[9] European Data Protection Board (2023). EDPB Work Programme 2023/2024. https://www.edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf

[10] SRB v. EDPS, (Court of Justice of the European Union April 26, 2023). https://gdprhub.eu/index.php?title=CJEU_-_Case_T-557/20_-_SRB_v._EDPS#:~:text=EDPS,-From%20GDPRhub&text=The%20European%20General%20Court%20ordered,alphanumeric%20codes%20constituted%20personal%20data.

[11] Infocomm Media Development Authority (n.d.). Privacy Enhancing Technology Sandboxes. Retrieved May 2, 2024, from https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes

[12] Infocomm Media Development Authority (n.d.). Digital Advertising in a Paradigm Without 3rd Party Cookies. Retrieved May 2, 2024, from https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--meta.pdf

[13] Kwon, S. (2024, February 2). In the era of artificial intelligence, standards for pseudonym processing for images, videos, voices, and texts have emerged. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=989

[14] OECD (2023).

[15] UN Committee of Experts on Big Data and Data Science for Official Statistics. (n.d.). Task Team on Privacy Preserving Techniques — UN GWG for Big Data. Unstats.un.org. Retrieved May 2, 2024, from https://unstats.un.org/bigdata/task-teams/privacy/index.cshtml

[16] Prorrogadas consultas sobre guia de anonimização e norma de direitos dos titulares (2024, February 28). Autoridade Nacional de Proteção de Dados. https://www.gov.br/anpd/pt-br/assuntos/noticias/prorrogadas-consultas-sobre-guia-de-anonimizacao-e-norma-de-direitos-dos-titulares