

REIMAGINANDO LA PRIVACIDAD EN LA ERA DE LA IA: **LA PRIVACIDAD DE LOS DATOS PERSONALES COMO BIEN PÚBLICO**

Un llamamiento a la responsabilidad compartida y a protecciones más sólidas para salvaguardar la privacidad del consumidor en la era digital.

LA INTELIGENCIA ARTIFICIAL ESTÁ HACIENDO QUE LAS OPCIONES DE PRIVACIDAD INDIVIDUAL SEAN INADECUADAS

Hace cincuenta años, los datos personales eran en gran medida privados por defecto.ⁱ Hoy en día, pueden compartirse, venderse o intercambiarse al instante, con o sin su consentimiento. El movimiento global de consumidores exige acciones urgentes para proteger la privacidad.

Los consumidores necesitan protecciones colectivas más sólidas para garantizar que los datos personales se utilicen de manera responsable, transparente y justa en la era de la IA.

La privacidad ya no puede gestionarse únicamente con decisiones individuales. Protegerla debe ser algo compartido, no una responsabilidad privada.

EL PROBLEMA: SE PIDE A LOS CONSUMIDORES GESTIONAR LOS RIESGOS SISTÉMICOS DE PRIVACIDAD

La privacidad se trata como responsabilidad de cada persona: leer extensos avisos de política, gestionar entornos complejos e intercambiar datos personales por servicios digitales.

Ese enfoque ya no refleja cómo la inteligencia artificialⁱⁱ (IA) usa los datos de los consumidores. Ahora, los sistemas de IA pueden predecir información sobre nosotros que nunca compartimos explícitamenteⁱⁱⁱ con consecuencias poco claras impulsadas por decisiones de diseño y falta de gobernanza. Los perjuicios podrían incluir más cobros, negación de crédito o seguro, orientación hacia opciones menos favorables o ataques en función de características inferidas. Los consumidores en circunstancias vulnerables suelen ser los más afectados y tienen menos vías de recurso.

90% de defensores del consumidor en todo el mundo identifican la privacidad y la seguridad como principales riesgos para consumidores derivados de la IA.^{iv}

NUESTRO LLAMADO: HACER DE LA PRIVACIDAD UNA PROTECCIÓN COMPARTIDA

Tratar la privacidad como un bien público – como el aire limpio o la seguridad vial – con protecciones que funcionen para todos en lugar de responsabilizar a las personas. Nuestro llamado a la acción establece seis principios, desarrollados junto con organizaciones de consumidores, para ayudar a avanzar en la defensa del consumidor, guiar prácticas empresariales responsables y apoyar una regulación más estricta.

El objetivo es sencillo: garantizar que nadie pueda usar nuestros datos para cobrarnos más, excluirnos injustamente o explotar nuestras vulnerabilidades.

Un enfoque de bien público no significa usar menos datos. Significa gestionar los datos a modo de maximizar el beneficio público y minimizar el daño.

LA RECOMPENSA: UNA PRIVACIDAD MÁS FUERTE GENERA CONFIANZA EN LA ECONOMÍA DIGITAL

La privacidad es un factor importante para fomentar la confianza y la seguridad en la economía digital. Sistemas transparentes, responsables y que rindan cuentas reducen riesgos, permiten un uso seguro y justo de los datos y empoderan a los consumidores para interactuar con confianza con los servicios digitales. Unas fuertes protecciones de la privacidad refuerzan la confianza del consumidor y ayudan a garantizar que la innovación aporte beneficios para todos.

A medida que la IA permite a los proveedores recolectar, predecir y utilizar cada vez más información, las preocupaciones sobre la privacidad de los datos personales siguen creciendo.

Los proveedores que protegen la privacidad pueden tener una ventaja competitiva, pero solo cuando los consumidores tienen oportunidades reales de elegir, cambiar y llevar sus datos a otro lugar.

Definición: Proveedor

Una organización que desarrolla u opera sistemas de datos a gran escala, usando datos personales para tomar decisiones, personalizar servicios o influir en los resultados de los consumidores.

¿QUÉ ES LA PRIVACIDAD Y QUÉ ES UN BIEN PÚBLICO?

PRIVACIDAD



significa poder controlar cómo su información y datos se recolectan, usan y comparten.^v

UN BIEN PÚBLICO



es un recurso o condición cuyos beneficios y peligros se comparten en toda la sociedad, lo que requiere una gobernanza colectiva, en vez de una gestión individual.

LOS BIENES PÚBLICOS TIENEN DOS CARACTERÍSTICAS CLAVE

NO EXCLUIBLES: las personas no pueden evitar ser afectadas.

NON-RIVALROUS: el beneficio de una persona no reduce los beneficios de otra.

	EXCLUIBLES	NO EXCLUIBLES
RIVALIZAN	BIENES PRIVADOS  comida  ropa  carros	BIENES COMUNES  pesca  madera  carbón
NO RIVALIZAN	BIENES DE CLUBES  cines  gimnasios  playas privadas	BIENES PÚBLICOS  aire limpio  seguridad vial

78% de consumidores en Estados Unidos apoyarían una ley que regule cómo las empresas pueden recolectar, almacenar, compartir y utilizar nuestros datos personales.^{vi}

EJEMPLOS DE BIENES PÚBLICOS



AIRE LIMPIO: Ninguna persona puede optar por no tener contaminación atmosférica, y la exposición de una persona no reduce la de otra. La sociedad depende de protecciones colectivas, como las normas de emisiones y las regulaciones de calidad del aire, en lugar de esperar que las personas gestionen el riesgo por sí mismas.



SEGURIDAD VIAL: Carreteras seguras, vehículos más seguros, límites de velocidad y leyes sobre el cinturón de seguridad protegen a todos, incluyendo aquellos que personalmente deciden prescindir de tales protecciones. El consentimiento individual no es el principio rector de la seguridad vial.



PRIVACIDAD no es un bien público de manual, pero cada vez funciona de la misma manera. La IA genera riesgos que afectan a todos, haciendo que las protecciones colectivas sean cada vez más necesarias.

SEIS PRINCIPIOS PARA LA PRIVACIDAD COMO BIEN PÚBLICO

Si la privacidad es una condición compartida y no una responsabilidad individual, necesitamos reglas compartidas que protejan a todos. Nuestro marco se basa en seis principios:

1 

LOS DATOS SIRVEN PRIMERO AL INTERÉS DEL CONSUMIDOR

Los proveedores deben utilizar los datos personales de manera que beneficie a los consumidores y sea consistente con el propósito para el cual se recopilaron.

2 

PROTEGER CONTRA EL PERFILADO DAÑINO DE LA IA

Proteger a las personas no solo contra la recolección excesiva de datos, sino también contra predicciones y perfiles dañinos.

3 

GARANTIZAR LA RENDICIÓN DE CUENTAS Y APLICACIÓN EFICAZ

La protección del consumidor debería integrarse en los sistemas, mercados y marcos regulatorios de IA, en lugar de depender de los individuos para salvaguardar sus propios derechos.

4 

PERMITIR UNA SALIDA FÁCIL, PORTABILIDAD Y ELECCIÓN REAL

Los consumidores deberían poder mover y eliminar sus datos sin obstáculos.

5 

EXIGIR PRE-PRUEBAS, MONITOREO E INTERVENCIÓN HUMANA

Los sistemas de IA deben ser probados, monitoreados y auditados antes y después del despliegue para establecer barreras de privacidad. Como los daños sistémicos pueden ser difíciles de detectar, la supervisión debería centrarse en resultados del mundo real, así como en el cumplimiento de los requisitos regulatorios.

6 

GARANTIZAR UNA SOLUCIÓN Y REPARACIÓN EFICACES PARA DAÑOS A LA PRIVACIDAD SUFRIDOS

Los consumidores deben poder comprender las decisiones, impugnar los resultados y obtener compensación oportuna cuando se producen daños a la privacidad.

PROTEGIENDO JUNTOS LA PRIVACIDAD DE LOS DATOS PERSONALES

La IA ha convertido la privacidad en un problema colectivo.



Muchos de los riesgos actuales para la privacidad son colectivos, más que individuales. Eso se debe a que la IA puede aprender cosas sobre ti a partir de información sobre otras personas similares a ti, incluso si nunca compartiste esa información tú mismo. Tratar la privacidad como bien público pone las responsabilidades de gobernanza en los actores más capaces de gestionar estos riesgos colectivos, en vez de dejar que los consumidores los afronten solos.

Los consumidores no pueden protegerse solos.



Incluso si no compartes tus propios datos, los proveedores pueden inferir información sobre ti a partir de los datos de tu familia, amigos o personas como tú. También ocurre lo contrario: tus datos pueden revelar información sobre otros que no han compartido nada ellos mismos. Por tanto, la privacidad es una condición compartida. Ninguna persona puede protegerla completamente —ni consentir que se retire— por sí misma.

Las empresas no pueden resolver el problema solas.



Aún empresas comprometidas con prácticas de privacidad más estrictas se enfrentan a un problema de acción colectiva. Actuar solo puede crear una desventaja competitiva si los rivales continúan extrayendo y monetizando datos excesivos de consumidores. Las reglas compartidas permiten a las empresas actuar juntas sin que ninguna de ellas pague el precio de ir primero.

¿POR QUÉ DEBERÍA TRATARSE LA PRIVACIDAD COMO UN BIEN PÚBLICO?

Los mayores daños recaen sobre los menos capaces de soportarlos.



La IA puede reforzar la discriminación, la manipulación y la clasificación injusta de los consumidores en una escala que ningún individuo puede identificar o disputar. Los consumidores en situaciones vulnerables suelen ser los más afectados, lo que amplifica las desigualdades existentes.^{vii}

La privacidad es cosa de justicia, no de secretismo.



La privacidad no se trata de tener algo que ocultar. Se trata de garantizar que la información personal no pueda usarse para cobrar más a las personas, excluirlas injustamente de oportunidades, manipular sus elecciones o explotar sus vulnerabilidades. Incluso datos aparentemente inofensivos pueden combinarse y analizarse para afectar la vida de las personas de formas que quizá nunca vean o comprendan.

La autogestión impone una gran carga para los consumidores.



Los modelos actuales de notificación y consentimiento esperan que los consumidores vigilen su privacidad en todos los servicios. En la práctica, muchos consumidores sienten que tienen pocas opciones significativas, pero para compartir sus datos y acceder a servicios digitales. La protección de la privacidad no debería depender de la vigilancia individual.

LA ECONOMÍA ACTUAL DE DATOS IMPULSADA POR IA EXPONE A LOS CONSUMIDORES A DAÑOS EN CADA ETAPA

PASO 1:

Los datos se recolectan para usos que van más allá de servir al consumidor.



Un modelo de negocio dominante trata los datos de los consumidores como materia prima que debe extraerse, procesarse y monetizarse más allá de lo que beneficia al consumidor. El intercambio de datos puede aportar beneficios reales, ya sea en estafas o prevención de fraude,^{viii} y los consumidores pueden valorar la personalización cuando sea adecuada. Sin embargo, recopilar más datos de los necesarios crea oportunidades de daño.

EJEMPLO: EL BANCO UTILIZA DATOS PARA DETENER ESTAFAS

Un banco detecta un pago inusual y detiene una estafa antes de que el dinero salga de la cuenta del cliente. Esto protege a los consumidores porque los datos se utilizan con un propósito claro. En contraste, recolectar, reutilizar y comerciar datos sin límites claros elimina esa protección. El valor para el consumidor requiere un propósito definido.

PASO 2:

Creación no autorizada de nuevos datos y perfiles del consumidor.



La IA toma los datos existentes del Paso 1 para generar nuevos perfiles de comportamiento y predicciones sobre las personas, incluyendo información que nunca compartieron explícitamente. Estas predicciones evolucionan a una velocidad y escala que superan los marcos de consentimiento individual y las salvaguardas existentes a menudo no regulan adecuadamente cómo se crean o utilizan estas predicciones.^{ix}

EJEMPLO: DATOS DE ESQUEMAS DE FIDELIDAD UTILIZADOS MÁS ALLÁ DEL CONSENTIMIENTO

Un consumidor se une a un plan de fidelización en un supermercado y acepta recibir ofertas personalizadas. Años después, los mismos datos de compra son utilizados por un sistema de IA para predecir características sensibles, como riesgos para la salud, estrés financiero o grandes cambios en la vida. El perfil resultante se comparte con terceros con los que el consumidor nunca esperó interactuar. Su consentimiento original no se extendía a la creación o el intercambio de este perfil conductual.

PASO 3:

Las decisiones opacas de IA afectan al acceso del consumidor a productos y servicios, con recurso poco claro.



Les prédictions faites lors de l'étape 2 peuvent influencer les prix, les produits et les opportunités, souvent à l'insu des personnes concernées et sans que celles-ci puissent contester le résultat.^x

EJEMPLO: CÁLCULO DE LA TASA HIPOTECARIA SIN EXPLICACIÓN

Un consumidor renueva su hipoteca y se le cotiza un tipo más alto del esperado. En lugar de basarse en factores tradicionales —como antigüedad, código postal, historial de reclamos— el sistema de precios de IA del prestamista analiza una amplia gama de datos para predecir riesgos y rentabilidad, lo que puede sacar conclusiones sobre el consumidor a partir de datos personales que nunca reveló. El consumidor no recibe una explicación clara para el tipo más alto y tiene pocas oportunidades de comprender, cuestionar o cuestionar el resultado.

CONSTRUYENDO UNA ECONOMÍA DIGITAL QUE PROTEJA A LOS CONSUMIDORES Y OFREZCA BENEFICIOS MÁS AMPLIOS

Un enfoque de bien público no significa que necesitemos menos datos. Significa gestionar los datos de manera que maximicen los beneficios para los consumidores minimizando el daño.

CONFIANZA Y PARTICIPACIÓN DIGITAL



Los consumidores deberían poder utilizar los servicios digitales sin sentir que tienen que ceder su privacidad a cambio. Unas sólidas protecciones básicas reducen la incertidumbre sobre cómo se recolectan, utilizan y comparten los datos personales. Cuando la privacidad está protegida por defecto, los consumidores pueden participar en la economía digital con mayor confianza.

EJEMPLO

Un consumidor puede asistir a un evento público o utilizar un servicio esencial sin que su presencia sea rastreada, perfilada o dirigida para fines comerciales no relacionados.

MERCADOS MÁS EFICIENTES



El marco de privacidad actual suele depender de que las personas identifiquen los problemas después de que ya se haya producido un daño. Un enfoque de bien público traslada la responsabilidad a proveedores y reguladores para prevenir daños desde el principio. Normas claras y rendición de cuentas crean mayor certeza tanto para consumidores como para empresas.

EJEMPLO

La seguridad alimentaria protege a todos los que compran alimentos, no solo a quienes leen las etiquetas. La privacidad de los datos debería funcionar igual, con protecciones integradas en el sistema en lugar de depender de que los consumidores gestionen cada riesgo por sí mismos.

MAYOR VARIEDAD E INNOVACIÓN



Hoy en día, los servicios con más usuarios suelen tener la mayor ventaja de datos: más datos pueden fortalecer los productos, mejorar la segmentación y reforzar el poder de mercado. Fuertes protecciones de privacidad, combinadas con una portabilidad efectiva y derechos de conmutación, pueden crear oportunidades para que los nuevos servicios compitan por calidad, confianza e innovación en lugar de por el volumen de datos que han acumulado.

EJEMPLO

Un proveedor que ofrece servicios de protección de la privacidad puede competir ganándose la confianza del consumidor, en lugar de recolectar cada vez más información personal.

CRECIMIENTO ECONÓMICO A TRAVÉS DE CONFIANZA



La confianza es una base de la economía digital. Sostenemos que cuando los consumidores creen que sus datos se utilizarán de forma responsable, están más dispuestos a interactuar con nuevas tecnologías y servicios. Las empresas se benefician de relaciones más sólidas con los clientes, mientras que los innovadores pueden desarrollar productos que generen valor sin depender de prácticas de datos cada vez más intrusivas. Las protecciones de privacidad compartidas también ayudan a garantizar que las empresas compitan en base a la confianza y la innovación, en lugar de en cuántos datos de consumidores pueden extraer.^{xi}

CÓMO PODEMOS LOGRAR ESTO: PRINCIPIOS FUNDAMENTALES DE LA PRIVACIDAD COMO BIEN PÚBLICO

Si la privacidad es una condición colectiva y no una responsabilidad individual, la gobernanza debería cambiar de gestionar las elecciones del consumidor para moldear el comportamiento de los proveedores y sistemas. Estos seis principios proporcionan un marco para hacerlo.^{xii}



PRINCIPIO 1: LOS DATOS SIRVEN EL INTERÉS DEL CONSUMIDOR ANTE TODO

Los proveedores deben utilizar los datos personales a modo que beneficien a los consumidores y sean coherentes con el propósito para el que se recolectaron los datos.

- **Estándares más elevados para personas con mayor riesgo.** Los sistemas de IA deberían aplicar protecciones más fuertes —como desactivar el perfilado y la segmentación y aplicar configuraciones de protección por defecto— al procesar datos relacionados con niños, consumidores mayores u otras personas que puedan ser más vulnerables a daños.
- **Trato justo de los datos, independientemente del consentimiento.** Toda recolección y uso de datos debe ser justo y proporcional, independientemente de si el consumidor ha dado su consentimiento o no. El consentimiento no puede autorizar un tratamiento injusto que genere daño o riesgo irrazonable, y el consentimiento de una persona no puede autorizar el tratamiento de los datos de otra.
- **Usar tecnologías que preservan la privacidad.** Los proveedores deberían priorizar enfoques que ofrezcan utilidad, incluyendo la personalización cuando sea relevante, sin requerir la recopilación masiva de datos personales. La tecnología ya lo hace posible.^{xiii}
- **Mantener estándares de seguridad estrictos.** Los proveedores deben mantener estándares de seguridad proporcionales a la sensibilidad de los datos que poseen y a la escala en la que operan. Un marco de privacidad que pueda ser socavado por una brecha prevenible no funciona para el interés público. Las obligaciones de seguridad deben ser continuas y auditables.



PRINCIPIO 2: PROTEGER CONTRA EL PERFILADO DAÑINO DE IA

Proteger a las personas no solo de la recolección excesiva de datos, sino también de predicciones y perfiles dañinos.

- **No se permite la reutilización automática de datos para el entrenamiento de IA.** Los datos recogidos con un solo propósito no deberían reutilizarse para entrenar sistemas de IA de formas que entran en conflicto con la legislación aplicable, obligaciones de privacidad, compromisos contractuales o expectativas razonables del consumidor. Estos usos deben estar regulados desde el punto de la recolección y sujetos a transparencia, proporcionalidad y supervisión.
- **Límites en los datos y perfiles predichos.** Las obligaciones deberían extenderse a lo que los sistemas de IA pueden predecir y actuar sobre lo que se permite, incluyendo el estado de salud, la vulnerabilidad financiera y los valores o creencias predichas a partir de otra información, no solo a los datos recolectados. Los límites deben ser proporcionados: cuanto mayor sea el impacto potencial en el acceso de los consumidores a servicios, empleos u otros resultados consecuentes, más fuertes deberían ser los controles.
- **Usos prohibidos y restringidos.** Ciertos usos de datos deberían prohibirse independientemente del consentimiento, incluyendo predecir características protegidas de manera que permitan discriminación ilegal, trato injusto, explotación o manipulación; segmentación basada en vulnerabilidad; o uso de perfiles conductuales para manipular la toma de decisiones.



PRINCIPIO 3: GARANTIZAR LA RENDICIÓN DE CUENTAS Y LA APLICACIÓN EFICAZ

La protección al consumidor debería estar integrada dentro de sistemas, mercados y marcos regulatorios de IA, en lugar de depender de los individuos para proteger sus propios derechos.

- **La exigibilidad requiere inversión.** Los organismos reguladores deben contar con la experiencia técnica, el mandato legal y los recursos necesarios para gobernar eficazmente los sistemas de IA.
- **La elección del consumidor y la protección de la privacidad deberían ser prioridades regulatorias.** Los marcos regulatorios deben garantizar que el poder de mercado no se utilice para dificultar el cambio de opinión de los consumidores o para debilitar la privacidad y la elección, a modo que esa escala beneficie a los consumidores en lugar de consolidar el control sobre sus datos.
- **Gobernanza transfronteriza.** Los estándares mínimos vinculantes para la recolección y procesamiento de datos deben aplicarse independientemente de la sede o de la tramitación de datos. La aplicación y el intercambio de información entre jurisdicciones deben respaldar protecciones consistentes.

CÓMO PODEMOS LOGRAR ESTO: PRINCIPIOS FUNDAMENTALES DE LA PRIVACIDAD COMO BIEN PÚBLICO



PRINCIPIO 4: PERMITIR UNA SALIDA FÁCIL, PORTABILIDAD Y UNA ELECCIÓN REAL

Los consumidores deberían poder mover y eliminar sus datos sin barreras.

- **Portabilidad y compatibilidad entre servicios.** La portabilidad de datos y, cuando sea apropiado, la interoperabilidad, pueden apoyar la elección, la innovación y la confianza del consumidor cuando se implementan de manera segura, protectora de la privacidad y proporcionada.^{xiv} Los consumidores deberían poder elegir los servicios que protegen mejor su privacidad sin quedar atrapados.
- **Eliminación simple de cuentas.** Los consumidores deberían poder cerrar una cuenta y que sus datos personales sean borrados mediante un proceso no más difícil que el utilizado para registrarse.
- **Retiro del consentimiento.** Cuando el procesamiento depende del consentimiento, los consumidores deberían poder retirarlo tan fácilmente como lo dieron, en cualquier momento y sin penalización.



PRINCIPIO 5: EXIGIR PRUEBAS PREVIAS, MONITOREO E INTERVENCIÓN HUMANA

Los sistemas de IA deben ser probados, monitoreados y auditados antes y después de su despliegue para mantener las barreras de privacidad. Dado que los daños sistémicos pueden ser difíciles de detectar, la supervisión debería centrarse en los resultados del mundo real, así como el cumplimiento de los requisitos normativos.

- **Evaluaciones pre-despliegue.** Los sistemas de IA utilizados en áreas de alto impacto, como la sanidad o los servicios financieros, deberían estar basados en evaluaciones basadas en riesgo antes del despliegue. La evaluación debe ser proporcional al caso de uso, la sensibilidad de los datos implicados y la gravedad y probabilidad de posibles daños.^{xv}
- **Intervención humana.** La supervisión humana debería permitir a los proveedores identificar, cuestionar y corregir los resultados perjudiciales.
- **Auditoría continua.** Los proveedores deben monitorear y auditar activamente los sistemas de IA a lo largo de su ciclo de vida. La auditoría y las pruebas deben identificar resultados discriminatorios, desplazamiento del sistema, impactos desproporcionados en grupos específicos y daños emergentes.
- **Informes de transparencia.** Las entidades reguladas deberían informar sobre el rendimiento de sus sistemas según los estándares requeridos, haciendo visibles los resultados para los reguladores y el público.



PRINCIPIO 6: GARANTIZAR REPARACIÓN EFICAZ Y COMPENSACIÓN POR LOS DAÑOS A LA PRIVACIDAD SUFRIDOS

Los consumidores deben ser capaces de comprender las decisiones, impugnar los resultados y obtener una compensación oportuna cuando se producen daños a la privacidad.

- **Un punto de contacto claro para los consumidores.** Cada jurisdicción debería tener un organismo designado con el mandato y recursos para proporcionar apoyo humano en denuncias, investigaciones y aplicación de la ley. Los consumidores deben saber a dónde acudir para pedir ayuda.
- **Decisiones que la gente puede entender y cuestionar.** Cuando la IA influye en decisiones trascendentes, los consumidores deberían recibir explicaciones en términos que los consumidores y reguladores puedan entender y seguir sobre los que puedan actuar.
- **La compensación debe coincidir con la magnitud del daño.** Cuando la IA perjudica a grandes grupos de consumidores, la compensación también debe operar a gran escala. Las organizaciones de consumidores y los reguladores deberían poder emprender acciones colectivas en nombre de todos los afectados, en lugar de dejar a los individuos buscar la solución por sí solos.^{xvi}

OFRECIENDO MEJORES RESULTADOS PARA LOS INTERESADOS

PARA CONSUMIDORES



Un enfoque de bien público significa que la protección de la privacidad ya no depende del consumidor individual, conocimiento, tiempo o recursos. Las personas están protegidas por el propio sistema. Esto:

- elimina la carga sobre las personas para gestionar riesgos sistémicos de privacidad;
- protege contra la explotación, independientemente de su capacidad o alfabetización digital;
- crea rutas significativas para desafiar las decisiones impulsadas por IA;
- promueve la elección y la interoperabilidad entre servicios;
- fortalece los sistemas de rendición de cuentas para los consumidores.

PARA EL SECTOR PRIVADO



Reglas claras benefician a las empresas. Esto:

- distingue entre el uso de datos que crea un valor genuino y prácticas que son simplemente extractivas;
- crea condiciones competitivas consistentes que se aplican en todo el mercado;
- construye la confianza del consumidor como un activo competitivo en el mercado en lugar de tratar la privacidad como un costo de cumplimiento.^{xvii}

PARA GOBIERNOS



Un marco de bien público proporciona a los gobiernos las herramientas para gobernar de forma proactiva, en lugar de responder después de que se haya producido un daño. Esto:

- cambia el enfoque de la aplicación reactiva a salvaguardas a nivel de sistema;
- refuerza la confianza pública en los sistemas digitales y en las instituciones que los supervisan;
- proporciona una base para la cooperación transfronteriza en un tema que no respeta fronteras nacionales.

UN LLAMADO COLECTIVO PARA RECONOCER LA PRIVACIDAD DE LOS DATOS PERSONALES COMO UN BIEN PÚBLICO



consumer.



BENIN SANTE ET SURVIE
DU CONSOMMATEUR
(BSSC)



消費者委員會
CONSUMER COUNCIL
香港 • HONG KONG



UN LLAMADO COLECTIVO PARA RECONOCER LA PRIVACIDAD DE LOS DATOS PERSONALES COMO UN BIEN PÚBLICO

CONSUMER VOICE



epic.org / ELECTRONIC
PRIVACY
INFORMATION
CENTER

FORBRUKERRÅDET

**FIJIAN
COMPETITION &
CONSUMER
COMMISSION**

idec
instituto de defensa
de consumidores



koodos



LEMBAGA KONSUMEN YOGYAKARTA
YOGYAKARTA CONSUMER INSTITUTE

မြန်မာစားသုံးသူများသမဂ္ဂ
**MYANMAR
CONSUMERS UNION**
Rights and Responsibilities thru Education



ONPECO
OBSERVATORIO NACIONAL
PARA LA PROTECCIÓN DEL CONSUMIDOR

**PARADIGM
INITIATIVE**

**Privacy
Foundation**

Proconsumer



**SVERIGES
KONSUMENTER**
THE SWEDISH CONSUMERS' ASSOCIATION

**SOUTH SUDAN
CONSUMER
PROTECTION
ORGANIZATION**



สภาองค์กรของผู้บริโภค
Thailand Consumers Council



TheNetwork
for Consumer Protection

TRIBUNAL
ECUATORIANA DE
CONSUMIDORES
Y USUARIOS

**VOICES OF
PRIVACY**



FIRMANTES

Reclamando la privacidad en la era de la IA: la privacidad de los datos personales como bien público es respaldada por las siguientes organizaciones:

ORGANIZACIÓN	PAÍS
Acción del Consumidor (ADELCO)	Argentina
Association for the Defence of Consumers and the Environment (ADEC - Association pour la Défense de l'Environnement et des Consommateurs)	Senegal
Benin Health and Consumers' Survival (BSSC - Bénin Sante et Survie du Consommateur)	Benín
Brazilian Institute of Consumer Protection (IDEC - Instituto Brasileiro de Defesa do Consumidor)	Brasil
Bulgarian National Association Active Consumers (BNAAC)	Bulgaria
Consumer Advocacy and Empowerment Foundation of Nigeria (CADEF)	Nigeria
Consumer Association of Mauritius (ACIM - Association des Consommateurs de l'Ile Maurice)	Mauricio
Consumer Council of Fiji	Fiji
Consumer Defence Association (ADECO - Associação para Defesa do Consumidor)	República de Cabo Verde
Consumer Defence Group of Mali (REDECOMA - Regroupement pour la défense des consommateurs du Mali)	Mali
Consumer Education and Research Centre (CERC)	India
Consumer NZ	Nueva Zelanda
Consumer Policy Research Centre (CPRC)	Australia
Consumer Protection Association of Mercosur (PROCONSUMER - Asociación de Protección de los Consumidores del Mercosur)	Argentina
Consumer Protection Association	Kuwait
Consumer Reports	Estados Unidos
Consumer Unity and Trust Society (CUTS)	India
Consumer VOICE	India
Consumers Association of Bangladesh	Bangladés
Consumers Council of Canada	Canadá
Consumers Japan	Japón
Electronic Privacy Information Center (EPIC)	Estados Unidos

ORGANIZACIÓN	PAÍS
Empower India	India
Federation of Consumers and Users (CECU - Federación de Consumidores y Usuarios)	España
Fijian Competition & Consumer Commission (FCCC)	Fiji
Fundación Ambio	Costa Rica
Hong Kong Consumer Council	Hong Kong
Kenya Consumers Organisation	Kenia
Koodos Labs	Estados Unidos
Myanmar Consumers Union	Myanmar
National Observatory for Consumer Protection (ONPECO)	República Dominicana
Norwegian Consumer Council (Forbrukerrådet)	Noruega
Privacy Foundation NZ	Nueva Zelanda
Paradigm Initiative	Nigeria
South Sudan Consumer Protection Organisation (SSCPO)	Sudán Meridional
Swedish Consumers' Association (Sveriges Konsumenter)	Suecia
Thailand Consumer Council	Tailandia
The Network for Consumer Protection	Pakistán
Tribune of Consumers and Users of Ecuador (Tribuna Ecuatoriana de Consumidores y Usuarios)	Ecuador
Tunisian Organisation to Inform the Consumer (OTIC - l'Organisation Tunisienne pour Informer le Consommateur)	Túnez
Voices of Privacy	Estados Unidos
Yayasan Lembaga Konsumen Indonesia	Indonesia
Yemen Association for Consumer Protection	Yemen
Yogyakarta Consumer Institute (Lembaga Konsumen Yogyakarta)	Indonesia

AGRADECIMIENTOS

Estamos agradecidos a los colegas de Consumers International que lideraron la redacción y desarrollo de este documento, entre ellos: Erin Parsons, Nandini Harihareswara, Alexandra Straessle, Stefan Hall y Brooke Kingsland.

Este documento fue desarrollado por Consumers International con la orientación y aportaciones de un Grupo Asesor de IA multiactor y varios socios externos. Las organizaciones participantes se enumeran a continuación. Agradecemos a todos los colaboradores por sus valiosas perspectivas y comentarios, señalando que los principios aquí presentados no reflejan necesariamente las opiniones individuales de todas las organizaciones implicadas.

ORGANISATION
Amazon.com, Inc.
Consumentenbond NL
Consumer Policy Research Centre (CPRC)
Consumer Reports
Danish Consumer Council
DuckDuckGo
Javier Ruiz Diaz
Jeannie Paterson, PhD
Koodos Labs
Que Choisir Ensemble
Visa, Inc.

Consumers International reúne a más de 200 organizaciones miembros en más de 100 países para empoderar y defender los derechos de los consumidores en todas partes. Somos su voz en foros internacionales de formulación de políticas y en el mercado global para garantizar que sean tratados de forma segura, justa y honesta.

Consumers International es una organización benéfica (nº 1122155) y una sociedad sin ánimo de lucro limitada por garantía (nº 04337865) registrada en Inglaterra y Gales.

consumersinternational.org

🐦 @consumers_int

📌 /consumersinternational

- i Rule, J, *Vidas privadas y vigilancia pública: control social en la era informática* (1974). Londres: Schocken Books.
- ii Para los fines de este informe, la inteligencia artificial (IA) se refiere a la capacidad cognitiva de los agentes máquina que imita la cognición humana al procesar información y ejecutar tareas para las que el agente máquina está entrenado. Banco Mundial, *Glosario GovTech*. Disponible en: <https://www.worldbank.org/en/programs/govtech/gtmi/gtmi-glossary>
- iii La industria de la publicidad digital mantiene taxonomías estandarizadas para clasificar a las personas y el contenido con el que interactúan, publicadas por Interactive Advertising Bureau (IAB) Tech Lab. La Taxonomía de Contenidos define aproximadamente 700 categorías que describen el tema de una página o app, mientras que la Taxonomía de Audiencia clasifica a los consumidores en más de 1500 segmentos objetivo según atributos demográficos, de interés e intención de compra, incluyendo datos sensibles que pueden compartirse, intercambiarse y sincronizarse entre servicios digitales. Estas categorías también pueden utilizarse para inferir características más específicas. IAB Tech Lab, *Taxonomía de Audiencia y Taxonomía de Contenidos*. Disponible en: <https://iabtechlab.com/standards/#taxonomies>
- iv Consumers International, *Encuesta Global de IA* (2025).
- v La obra fundamental de Alan Westin de 1967 definió la privacidad como “la pretensión de individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida se comunica la información sobre ellos.” Westin, A, *Privacidad y libertad* (1967). Nueva York: Atheneum.
- vi Consumer Reports, *Encuesta sobre experiencias americanas: una encuesta multimodal representativa a nivel nacional* (2024). Disponible en: https://article.images.consumerreports.org/image/upload/v1728423752/prod/content/dam/surveys/Consumer_Reports_AES_September_2024.pdf
- vii Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), *Recomendación sobre la ética de la inteligencia artificial* (2022). Disponible en: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- viii Consumers International, *Deteniendo las estafas en línea: Fomentando la coherencia y la coordinación para los consumidores* (2026). Disponible en: <https://www.consumersinternational.org/media/699948/consumers-international-stopping-online-scams-building-consistency-and-coordination-for-consumers.pdf>
- ix Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), *El derecho a la privacidad en la era digital: informe* (2021). Disponible en: <https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>
- x Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), *Inteligencia artificial y protección del consumidor* (2024), p.12-13. Disponible en: https://unctad.org/system/files/information-document/ccpb_artificial_intelligence_consumer_protection_en.pdf
- xi Organización para la Cooperación y el Desarrollo Económicos (OCDE), *La intersección entre la competencia y la privacidad de los datos* (2024). Disponible en: https://www.oecd.org/en/publications/2024/06/the-intersection-between-competition-and-data-privacy_b5ac1ae6.html
- xii Estos principios escalan con el tamaño, el riesgo y el impacto: los principios aplicados a un proveedor dominante que procesa datos sensibles a gran escala no son los mismos que los aplicados a un proveedor pequeño o a un uso de bajo riesgo.
- xiii Se pueden construir sistemas para aprender patrones sin recopilar los datos de cada persona de forma centralizada, para responder preguntas útiles sin exponer a ningún individuo y para mantener información sensible en el propio dispositivo del consumidor. Por ejemplo, el aprendizaje federado entrena un modelo a través de muchos dispositivos u organizaciones para que solo las lecciones aprendidas vuelvan al desarrollador, no los datos personales subyacentes. La privacidad diferencial añade una cantidad calibrada de ruido a los resultados, de modo que los patrones útiles permanecen visibles mientras no se puede identificar a una sola persona. El procesamiento en el dispositivo mantiene el análisis en el propio teléfono u ordenador del consumidor, por lo que la información sensible nunca llega a los servidores de la empresa. Oficina del Comisionado de Información (ICO), *Guía sobre Tecnologías para Mejorar la Privacidad* (2023). Disponible en: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/>
- xiv Iniciativa de Transferencia de Datos, *Un camino a seguir para la portabilidad de la IA* (2025). Disponible en: <https://dtinit.org/blog/2025/08/26/path-forward-AI-portability>
- xv Cabe señalar que varios de los temas tratados en este principio están cubiertos por la regulación actual de la UE.
- xvi La compensación del consumidor incluye tener derechos y responsabilidades claramente comunicados y canales de reclamación accesibles. Debe garantizarse una resolución rápida mediante esquemas de reparación obligatoria que pongan la responsabilidad en quienes mejor estén posicionados para gestionar un riesgo determinado.
- xvii CGAP, *¿Es buena la privacidad de los datos para los negocios?* (2023). Disponible en: <https://www.cgap.org/research/publication/is-data-privacy-good-for-business>