https://www.elcorreo.eu.org/Datos-que-valen-millones-Quien-los-tiene-quien-los-vende

Derechos del siglo XXI: Datos que valen millones: ¿Quién los tiene, quién los vende?

- Imperio y Resistencia - Ingerencias, abusos y saqueos -

Fecha de publicación en línea: Martes 5 de mayo de 2026

Copyright © El Correo - Todos derechos reservados

Cada búsqueda en Google, cada compra *online*, cada desplazamiento con el teléfono en el bolsillo produce datos que alguien recolecta, procesa y vende. Mientras el mundo se fragmenta entre tres grandes modelos de gobernanza digital, el país sigue sin actualizar sus reglas.

Hay una distancia evidente entre el marco legal vigente y los desafíos que plantea el ecosistema digital.

Cada búsqueda en [toda plataforma] *Google*, cada compra *online*, cada desplazamiento con el teléfono en el bolsillo produce datos que alguien recolecta, procesa y vende. Argentina tiene una ley de protección de datos que cumple 25 años y no menciona siquiera la palabra « privacidad ». Mientras el mundo se fragmenta entre tres grandes modelos de gobernanza digital, el país sigue sin actualizar las reglas.

Recurso estratégico

Durante décadas, el petróleo fue el emblema del recurso estratégico que estructuraba el poder global. Hoy, ese lugar lo ocupan los datos: que se recolectan, procesan, almacenan y comercializan. Hay empresas cuyo modelo de negocio entero descansa sobre ellos. Y, a diferencia del petróleo, los datos los producen gratuitamente quienes menos se benefician de ellos: los usuarios.

Esta es la paradoja central del mercado de datos contemporáneo. La información es generada por individuos en sus interacciones cotidianas —búsquedas, compras, desplazamientos, conversaciones— pero administrada y monetizada por organizaciones con capacidades tecnológicas infinitamente superiores. El resultado es una asimetría estructural de poder que el derecho y la tecnología todavía no han logrado resolver.

El sociólogo Manuel Castells describió hace más de dos décadas la emergencia de una « sociedad informacional », no simplemente una sociedad con más información, sino una nueva forma de organización social basada en la capacidad de producir, procesar y transmitir datos en tiempo real a través de redes interconectadas.

En esa arquitectura, las organizaciones —empresas, plataformas, Estados— concentran los recursos tecnológicos, mientras los individuos generan permanentemente el insumo fundamental. Esa asimetría constitutiva es el punto de partida de todos los debates contemporáneos sobre gobernanza digital.

Mercado de datos

El mercado de datos no surgió con las redes sociales. Su historia comienza en los años setenta, cuando las empresas de *marketing* directo empezaron a construir bases de datos con información demográfica básica para segmentar potenciales consumidores. Era un mercado de intercambio de información simple: listas, registros, perfiles rudimentarios.

En los ochenta y noventa, la irrupción de los códigos de barras y los escáneres de punto de venta transformó el comercio minorista: de pronto era posible recolectar datos transaccionales masivos en tiempo real. Aparecieron los primeros data *brokers* —empresas dedicadas exclusivamente a recolectar, clasificar y comercializar información personal—, que construían perfiles combinando registros públicos, encuestas, historiales financieros y bases de datos comerciales.

Copyright © El Correo

La consolidación definitiva llegó con Internet. Google, Yahoo!, eBay, etc. y luego las redes sociales normalizaron un modelo de negocio que hoy parece obvio pero que representa una transformación radical: los usuarios acceden a servicios sin pago monetario mientras las plataformas monetizan los datos obtenidos.

En este marco, la socióloga Shoshana Zuboff bautizó este fenómeno como « capitalismo de vigilancia », que es un sistema donde las personas pierden el control sobre su propia conducta porque sus datos son extraídos mediante mecanismos que muchas veces no pueden entender, ni consentir de forma genuina.

Riesgos que nadie explica

La escala actual del procesamiento de datos introduce riesgos que van mucho más allá de la publicidad segmentada. El *Big Data* —caracterizado por volúmenes que superan la capacidad de las bases de datos convencionales, por la velocidad de generación y procesamiento en tiempo real, y por la variedad de formatos: texto, imagen, video, audio— desafía las infraestructuras regulatorias pensadas para otro mundo.

El **Machine Learning**, la herramienta analítica central de este ecosistema, puede descubrir patrones no lineales en grandes masas de datos sin hipótesis previa, lo cual lo hace extraordinariamente poderoso, pero también extraordinariamente opaco.

En este sentido, los sistemas de aprendizaje automático operan como « cajas negras » donde es difícil explicar por qué se tomó una decisión. Cuando esas decisiones determinan el acceso al crédito, la selección laboral o qué contenidos políticos ve cada ciudadano, la opacidad deja de ser un problema técnico y se convierte en un problema democrático.

Es en este marco en el que se hace relevante contar con mecanismos de gobernanza de datos, ya que éstos pueden adolecer de problemas desde su recopilación, como información defectuosa, sesgada, incompleta, lo que puede llevar a las organizaciones a operar con lo que se llama « arquitecturas espagueti », que son silos de información desconectados que generan desconfianza y altos costos. Y esa ineficiencia no es solo económica, sino que también es un riesgo para los individuos sobre quienes se toman decisiones basadas en datos de mala calidad.

Tres modelos

El panorama global de la gobernanza de datos está fragmentado en tres grandes arquetipos, cada uno con una filosofía distinta sobre quién debe controlar la información y para qué.

El modelo estadounidense opera bajo una lógica de mercado. Los datos son un activo que puede producirse, valorarse e intercambiarse libremente. La regulación es sectorial y los estándares los define la propia industria. El resultado es el ecosistema de plataformas más poderoso del mundo, y también el menos regulado en términos de protección individual.

La Unión Europea eligió el camino opuesto: los datos personales son un derecho inalienable, no una propiedad comercial. *El Reglamento General de Protección de Datos* (GDPR), vigente desde 2018, otorga a los ciudadanos el derecho a saber qué datos existen sobre ellos, a corregirlos, a portarlos y a exigir que sean eliminados. Las multas por incumplimiento pueden alcanzar el 4% de la facturación global de una empresa. Es el marco regulatorio más

Copyright © El Correo

ambicioso del mundo, aunque también el más complejo de implementar.

China opta por el control estatal: los datos son un recurso público esencial para la estabilidad y el desarrollo nacional, gestionado de forma centralizada. Las autoridades no solo acceden a los datos, sino que pueden obligar a su recolección para alimentar sistemas como el de Crédito Social. La « soberanía cibernética » implica que los datos solo pueden entrar o salir del país con permiso expreso del gobierno.

Una ley de 25 años

El principal instrumento legal argentino en materia de datos es la Ley 25.326 de Protección de Datos Personales, sancionada en el año 2000. Su objetivo es proteger los datos asentados en archivos y bancos de datos para garantizar el derecho al honor y a la intimidad.

El problema es que la ley tiene 25 años y no menciona explícitamente la « privacidad de datos personales ». Fue diseñada para otro mundo tecnológico, anterior al *Big Data*, al *Machine Learning* y a las plataformas digitales tal como las conocemos hoy.

De esta manera, la norma es reactiva más que preventiva, ya que suele aplicarse una vez que el daño ya ocurrió, funcionando más como mecanismo de reclamo que como estándar de prevención. La responsabilidad de activarla recae sobre el propio individuo afectado, que debe iniciar las acciones legales correspondientes. Y no existe un marco metodológico estandarizado que indique a las organizaciones cómo proteger los datos técnica y operativamente antes de usarlos.

Las consecuencias de estas brechas regulatorias no son abstractas. La suspensión del sistema de reconocimiento facial en la Ciudad de Buenos Aires, tras cuestionamientos por el acceso indebido a datos biométricos de millones de personas; las filtraciones masivas que afectaron al PAMI en 2023; los ataques a servidores del Poder Judicial de Chaco en 2022; y el uso de la aplicación CuidAR durante la pandemia —que habilitó la recolección masiva de datos con fines sanitarios— expusieron tensiones aún no resueltas entre innovación, seguridad, vigilancia y consentimiento.

En conjunto, estos casos muestran la distancia entre el marco legal vigente y los desafíos que plantea el ecosistema digital argentino.

En el plano institucional, la *Agencia de Acceso a la Información Pública* (AAIP) es el organismo de control. Más recientemente, la Disposición 2/2023 de la Subsecretaría de Tecnología de la Información aprobó una serie de recomendaciones para una Inteligencia Artificial Fiable, buscando promover la protección de datos desde una perspectiva ética. Son pasos, aunque insuficientes frente a la velocidad del cambio tecnológico.

Lo que falta

La brecha entre el marco legal vigente y las demandas del ecosistema digital contemporáneo es estructural. Actualizar la norma, construir capacidades institucionales y desarrollar estándares técnico-operativos obligatorios son tareas pendientes que requieren atención urgente.

Pero la discusión no es solo técnica. Detrás de cada modelo de gobernanza hay una decisión política: quién controla los datos, quién extrae valor económico de ellos, qué responsabilidades tienen las organizaciones respecto de la información que reciben y cuáles son los límites legítimos para el uso de datos personales. Esas preguntas no

Copyright © El Correo

tienen respuesta técnica, requieren deliberación democrática.

En un mundo donde la fragmentación global de las reglas de gobernanza plantea nuevos desafíos para la interoperabilidad y para la protección transfronteriza de derechos, Argentina no puede darse el lujo de seguir operando con una ley del año 2000. Avanzar en esa dirección no es solo una cuestión de eficiencia económica, es una condición para garantizar derechos fundamentales en la sociedad informacional del siglo XXI.

Ana Laura Jaruf* para **Página 12**

Página 12. Buenos Aires, 31 de mayo de 2026

Ana Laura Jaruf** es Magíster en Economía (UBA) e investigadora en el Centro Cultural de la Cooperación. Este artículo está basado en su trabajo académico « ***Mercado de Datos, desafíos y marcos regulatorios » (2026).