

EL COMPROMISO ÉTICO DE LA ADMINISTRACIÓN PÚBLICA PARA AFRONTAR LAS
COMPLEJIDADES DEL CUIDADO DE LOS DATOS PERSONALES
THE ETHICAL COMMITMENT OF MEXICAN PUBLIC ADMINISTRATION TO ADDRESS
THE COMPLEXITIES OF PERSONAL DATA CARE

DIEGO PAUL ÁLVAREZ MONTES¹ 

¹Universidad La Salle Bajío, León, Guanajuato, México

✉ Correspondencia: diego.alvarez.montes@hotmail.com

Recepción: 11 de abril de 2024 / Aceptación: 25 de mayo de 2024

SUMARIO

I. Introducción. II. Aspectos generales para el diseño institucional del cuidado de los datos personales. III. Conclusión. IV. Referencias

37

Resumen: El siguiente trabajo examina los desafíos que enfrenta la administración pública en la protección ética de los datos personales de los ciudadanos. Se destacan obstáculos administrativos e institucionales que obstaculizan la creación de un marco institucional sólido para salvaguardar la información personal. Se proponen acciones para abordar estos desafíos, apoyadas en la perspectiva de la gobernanza, con el fin de promover la corresponsabilidad de organismos públicos, privados y la sociedad en general en la protección de la información. Estas propuestas se fundamentan en la idea de que el cuidado de los datos es un principio democrático esencial para preservar la libertad y la autonomía de los ciudadanos en su interacción con el mundo digital.

Palabras clave: ética; democracia; datos personales; gobierno; gestión pública; gobernanza; modelos de gestión; gobiernos locales; organizaciones; instituciones.

Abstract: This document examines the challenges facing public administration in the ethical protection of citizens' personal data. Administrative and institutional obstacles hindering the establishment of a robust institutional framework to safeguard personal information are highlighted. Actions are proposed to address these challenges, supported by a governance perspective, aiming to promote the shared responsibility of public, private, and societal entities in protecting information. These proposals are grounded in the idea that data care is an essential democratic principle for preserving citizens' freedom and autonomy in their interaction with the digital world.

Keywords: ethics; democracy; personal data; government; public management; governance; management models; local governments; organizations; institutions.

I. Introducción

La mayoría de los ciudadanos se relaciona por los menos con una rutina que involucre la utilización del internet y el tratamiento de datos personales en plataformas digitales. Desde el pago de servicios públicos y privados, a través del celular, la compra de alimentos en plataformas digitales y la vinculación de cuentas bancarias por aplicaciones. Estos nuevos hábitos, ocasionados por las constantes provocaciones económicas para dar paso a la era de la modernidad digital, han evidenciado el avance en torno a los organismos privados que se adaptan ante estos escenarios de la globalización. Construyen plataformas y páginas digitales de manera que dan respuesta a las circunstancias y se adaptan a la dinámica del mercado, pero que no necesariamente se comprometen con el cuidado de la información.

Los hábitos en el uso de plataformas digitales, ya sea de consumo de productos o la pertenencia a un grupo o red social, implica relaciones esporádicas en las que difícilmente se percibe el riesgo de arrojar datos personales para la interacción con otras personas. De esta manera, estas relaciones esporádicas se manifiestan, por ejemplo, en compartir un mismo correo electrónico para todas las cuentas, e incluso, compartir una misma contraseña, por mencionar algunos aspectos. Se considera esporádica, ya que satisface una necesidad de determinado momento y vuelve a ser utilizado cuando esa necesidad se manifiesta; a pesar de esto, el arrojado de información personal pasa a un segundo plano sin considerar que se mantiene de manera permanente.

Es claro que los patrones de comportamiento social han cambiado, e incluso las manifestaciones de comunicación, apego y convivencia dependen en ocasiones de los medios digitales. A partir de esto, se han manifestado una serie de actos que han atentado contra la integridad de las personas, como las extorsiones, las calumnias, las mentiras, las opiniones con dolo, entre otros, de manera que se ha convertido en una arena digital en la que también involucra el uso de datos personales, los cuales son utilizados para realizar daño a otras personas.

Este documento resalta la preocupación de las fragilidades institucionales en las que operan los gobiernos, y así guiar con propuestas la realización de políticas públicas que regulen y cuiden el uso de los datos personales otorgados a organismos privados y a personas particulares, ya que desde luego repercute en la calidad de la democracia al no garantizar el cuidado de nuestra integridad, de este modo se disminuye el fortalecimiento de la confianza entre instituciones a partir de ambientes inscritos en la ética.

¿Por qué relacionar el cuidado de los datos de las personas como parte del compromiso con la democracia?

El auge de la tecnología ha llevado a un aumento significativo en la recopilación y explotación de datos personales por parte de empresas privadas, lo que afecta la privacidad de los ciudadanos y provoca que las empresas lucren con información sensible sobre hábitos de consumo, preferencias, ubicaciones geográficas, por mencionar algunos. Además, la tecnología ha mostrado nuevas formas de relacionarse socialmente sin la necesidad de interactuar físicamente. Estos hábitos que se interiorizan en nuestras formas de convivencia generan preocupación en el uso discrecional de la información personal, ya que atenta directamente contra los principios democráticos, pues socavan los valores de igualdad y libertad que son fundamentales para el funcionamiento de una

sociedad democrática. Los lazos de confianza pasan a un segundo plano y manifiestan las características de una modernidad en la que la lealtad, vinculada al respeto de la información personal de otras personas, se convierte en una acción innecesaria para convivir. Estos patrones de comportamiento cuestionan a las instituciones que le habían dado sentido a nuestra sociedad, las cuales se consideran para este documento como el tipo de estructuras que más importan en la esfera social, lo que implica que gran parte de la interacción y de la actividad humana está estructurada en términos de reglas explícitas o implícitas¹. El cuestionamiento a nuestros tradicionales hábitos de convivencia y de consumo ha generado retos normativos, administrativos y políticos en los gobiernos para afrontar estas nuevas formas de interactuar y con ello mantener las bondades de vivir bajo los regímenes democráticos.

A los gobiernos les ha costado tiempo y recursos descifrar cómo poder llevar a cabo políticas y protocolos de atención para el cuidado de los datos personales. En algunas ocasiones, no terminan de conectar ante una sociedad que minimiza la razón de inculcar una cultura de cuidado de la información, en otras ocasiones, la confianza en las instituciones se ve amenazada cuando los ciudadanos perciben que sus datos son utilizados fuera de los alcances por los que fueron recolectados.

Las manifestaciones en los cambios institucionales de convivencia también implican que, recoger datos personales, incentive la segregación poblacional al estratificar a las personas por categorías sociales, económicas y académicas, generando espacios de exclusión en el ofrecimiento de bienes y servicios tanto públicos y privados, y rechazando por ejemplo a aquellos que no estén en las circunstancias económicas para acceder a grupos económicamente posicionados, o segregados de espacios sociales por no ser del interés de quienes recogen la información. Estos actos pueden influir en la oferta de productos, oportunidades de empleo y otros aspectos de la vida cotidiana. Así, se destaca el enorme reto de coordinación institucional en el diseño y mejoramiento de entramados organizacionales, legislativos y administrativos para la protección de la privacidad e integridad de las personas.

II. Aspectos generales para el diseño institucional del cuidado de los datos personales

La coordinación de una estrategia gubernamental en materia de protección de datos personales requiere una estrategia integral que aborde temas relacionados con la ética, el desarrollo organizacional, las relaciones inter e intragubernamentales, con el fin de fortalecer un catálogo de acciones para que los organismos públicos atiendan las problemáticas relacionadas al tema, por ejemplo: la transferencia de datos a terceros, aclarar el papel del consentimiento del titular de la información y el tratamiento de datos sensibles, precisando espacios tanto físicos como digitales.

Es importante establecer un marco regulatorio y con perspectiva ciudadana que defina los procedimientos y obligaciones, tanto para el responsable como para los terceros receptores de los datos. La intención es detallar los roles que juegan organismos públicos, privados y ciudadanos ante el tema. Esto incluye la comunicación efectiva del aviso de

¹ Hodgson, Geoffrey, «¿Qué son las instituciones?», *Revista CS*, Colombia, num. 8, julio-diciembre de 2011, pp. 17-53.

privacidad a los terceros involucrados, asegurando que estén plenamente informados sobre las finalidades del tratamiento de los datos y las condiciones bajo las cuales se llevarán a cabo la transferencia de datos. Además, es esencial garantizar que los terceros receptores asuman las mismas responsabilidades que el responsable original, promoviendo así una cultura de responsabilidad compartida en el manejo de la información personal. El diseño del aviso de privacidad, en muchas ocasiones, se percibe como un documento *contractual* en lugar de una declaratoria de corresponsabilidad cívica. Esto se observa por ejemplo, en los contextos de lo privado, en el que algunas páginas de internet de empresas se reservan el acceso y uso de sus espacios informativos hasta la autorización del aviso de privacidad, independientemente de si se está de acuerdo o no. Caso contrario a los espacios físicos gubernamentales, en los que comúnmente se desconoce la importancia de generar estos documentos de aviso de privacidad y de que el intercambio de información se da en escenarios inciertos y con alto contenido de reglas informales.

Otro aspecto importante es la socialización del proceso de consentimiento de otorgar la información del titular a partir de ideas claras y explícitas en todos los casos. Como parte del compromiso ético, el acompañamiento gubernamental debe distinguirse con la misma voluntad tanto en etapas tempranas y maduras del otorgamiento y el uso de la información personal. El ciudadano tiende a no dimensionar que la protección debe garantizarse desde el inicio de la solicitud hasta el resguardo de los datos, ya que la idea es identificarlo como un derecho, puesto que sin su consentimiento, la información no pueda ser compartida. Para ello, es necesario establecer mecanismos eficaces para que los titulares puedan otorgar, modificar o revocar su consentimiento en cualquier momento, sin que esto tenga efectos retroactivos. Esto implica proporcionar información clara y accesible sobre cómo ejercer estos derechos, así como establecer procedimientos ágiles y eficientes para gestionar las solicitudes de los titulares.

En tercer lugar, en el caso de los datos personales sensibles, deberán garantizarse los medios de autenticación adecuados para verificar su identidad y asegurar la validez del consentimiento. Esto puede incluir diversas estrategias administrativas como la firma autógrafa, el fortalecimiento de la firma electrónica u otros mecanismos de autenticación reconocidos legalmente. La idea anterior es importante, ya que las burocracias tienden a neutralizar aquellas intenciones de modernización administrativa por razones de incertidumbre. Se han manifestado intenciones de modernización en la administración pública, como por ejemplo la digitalización de documentos y archivos públicos, así como la fijación de temporalidades de documentos para considerarlos posteriormente como obsoletos. La poca modernización administrativa, así como los obstáculos burocráticos para adaptarse a nuevas tendencias de organización, genera por el contrario, menor control de la información que se utiliza y con ello se expone las carencias institucionales para detener informalidades en el manejo de datos.

Con todo lo anterior, a continuación se propone una serie de ideas que involucra a la esfera gubernamental, en concreto para los poderes ejecutivo y legislativo, a fin de garantizar una coordinación estratégica de normas e instituciones para fortalecer el cuidado de la información personal: 1) salvaguardar los datos personales como principio ético universal; 2) fortalecer el cuidado de la democracia a partir de una corresponsabilidad compartida; 3) actualizar la normativa que involucra el tratamiento

de datos para operar estrategias administrativas; 4) sensibilizar a las empresas privadas sobre su compromiso del tratamiento de la información como un principio ético y, 5) descentralizar la acción administrativa. Este último, se suma como elemento clave para incentivar trabajos coordinados en las administraciones públicas. A partir de ello, se generarían las bases administrativas para desarrollar políticas públicas que defiendan al ciudadano ante acciones que repercuten su integridad y que a continuación se proponen sus detalles.

1) Salvaguardar los datos personales como principio ético universal. Reconocerlo como un principio ético, refuerza el compromiso tanto de la sociedad como del gobierno, para identificar a las personas como sujetos vulnerables ante el uso desconocido de nuestra información personal. El compromiso ético inicia desde la recopilación, el uso y la divulgación de datos hacia un tercero, esto implica también proteger a las personas contra el abuso de poder que pudiera representar. A su vez, el principio ético debe garantizarse por parte de quien comparte su información personal, al ser consciente de la existencia de espacios digitales que rompen con los acuerdos de protección de información y que pueden repercutir en los círculos cercanos de quien comparte, es decir, el uso indiscriminado de la información personal, repercute el contexto familiar, laboral, académico de donde se desenvuelve la persona. Por ello, tratar los datos personales como parte de los principios éticos, implica reconocer nuestra corresponsabilidad por proteger los contextos directos e indirectos de quienes comparten información, tener el hábito de verificar las páginas de internet y medios de consulta, con el fin de no exponer nuestras rutinas de vida.

41

2) Fortalecer el cuidado de la democracia a partir de una corresponsabilidad compartida. Como se ha mencionado, el cuidado y la vigilancia de los principios democráticos no es responsabilidad exclusiva de los gobiernos o las instituciones, sino que requiere de la participación activa de los ciudadanos. Es sumamente importante crear ciudadanía en las sociedades, y con ello fortalecer el espíritu crítico en el uso de la información como un tema complejo que involucra a la sociedad. Al ser un tema intangible, comúnmente la ciudadanía jerarquiza otro tipo de necesidades, algunas de corte económico, social y laboral, por lo que la información no ha terminado de comprenderse socialmente como un recurso que se conduce como medio para cumplir fines, es decir, se convierte en medio de intercambio para obtener beneficios dadas las influencias economicistas.

Basta con observar la enorme cantidad de actividades laborales y empresariales que han proliferado con la generación de información, clasificación o intercambio de datos con otros actores. Estas *nuevas* acciones han rebasado la capacidad institucional para afrontar las dinámicas laborales y económicas emergentes. Esto a su vez genera una asimetría de la información para quienes comparten sus datos, ya que no comprenden el impacto que hay al proporcionarlos. Sin duda, la protección de datos debe vigilarse desde una perspectiva democrática, dado que la información es un derecho para la ciudadanía. Asimismo, preservar la integridad es otro compromiso que los organismos públicos deberán tratar desde una perspectiva ciudadana.

El cuidado de la información debe comprenderse como una necesidad básica en la sociedad al socializar su importancia a nivel individual. Al participar activamente en la vigilancia, la sociedad se involucra en la observación de los comportamientos éticos de organismos públicos y privados, siendo así conscientes de las repercusiones que implica no cuidar nuestra información personal.

3) Actualizar la normativa que involucra el tratamiento de datos para operar estrategias administrativas. En la era digital actual, se ha convertido en una exigencia administrativa gestionar el tratamiento de información de las organizaciones públicas y privadas. La tecnología y la información han reforzado este objetivo, para que cualquier organismo —en al menos un proceso— considere el uso de la información a fin de cumplir con sus propósitos organizacionales. En los ámbitos público y privado, el manejo adecuado de los datos juega un papel fundamental en el éxito y la eficiencia de las estrategias administrativas. A pesar de observarse como ventaja económica, el rápido avance de la tecnología y los cambios en las prácticas comerciales han generado una creciente complejidad y nuevos desafíos en la gestión y el cuidado de los datos. Por lo tanto, la actualización de la normativa que regula el tratamiento de datos es esencial, y deberá convertirse en un hábito constante. La actualización del marco normativo genera las bases para consolidar estándares claros para la protección de la privacidad y los derechos individuales.

4) Sensibilizar a las empresas privadas sobre su compromiso del tratamiento de la información como principio ético. Las empresas privadas han convertido la información en un activo que potencializa la utilidad y proyección de sus respectivos objetivos. Cada vez aumentan los departamentos de las empresas que destinan áreas exclusivamente al manejo de datos, redes sociales, tendencias en el consumo de las personas, detección de necesidades entre otros aspectos. Las empresas han observado que con la información pueden obtener mayores beneficios. Sin embargo, la relación entre empresa y cliente no debe reducirse a una situación de transacción económica, sino que también debe comprender un compromiso ético en el que se trate a los ciudadanos como agentes, que en algunas circunstancias, comparten su información para obtener un producto.

La potencialización del uso de la información en las empresas ha impulsado estrategias de marketing en las que interactuar personalmente con otra persona no sea necesariamente un requisito para llevar a cabo una transacción económica. La pérdida de los lazos sociales, en plataformas económicas de este tipo, conlleva que la persona —convertida en cliente— esté exponencialmente expuesta respecto a las empresas o los establecimientos, en general. El intercambio de información no se genera bajo las mismas circunstancias ni condiciones, lo que ocasiona la proliferación de un sinnúmero de ejemplos en la que los organismos privados atienden dichas necesidades, manteniendo algunas empresas mayor empatía por el tema respecto a otras. El aumento exponencial de plataformas digitales, para llevar a cabo actividades económicas, constituye un gran reto para el fortalecimiento normativo. Las empresas dan pasos adelantados en el tema, en las que incluso se benefician ante el reducido entramado institucional que proteja los intereses de los consumidores.

Las empresas deberán reforzar su compromiso con el ciudadano más allá de una lógica clientelar, de esta manera no solo se fortalecería la interacción económica, sino que además las empresas se comprometerán en formar parte del entramado institucional que salvaguarda la información de sus clientes actuando bajo principios éticos. El manejo ético de los datos es esencial para construir y mantener la confianza del cliente, así como para garantizar el cumplimiento legal y la sostenibilidad a largo plazo. Sensibilizar a las empresas privadas sobre su compromiso con el tratamiento ético de la información no solo es una responsabilidad social, sino también una necesidad estratégica y comercial.

5) Descentralizar la acción administrativa. Parte de los retos de la administración pública, en torno al cuidado de la información, se encuentra en la construcción de una burocracia que garantice la vigilancia del cuidado de los datos personales. Se ha mencionado anteriormente la importancia del entramado institucional, concebida como la serie de reglas en las que permita que una situación se suscite o no bajo la vigilancia de acciones administrativas, políticas, económicas y/o sociales. Dada la herencia que ha marcado el actuar gubernamental en el sistema político mexicano, las acciones administrativas tienden a centralizar las decisiones políticas, marcando una serie de hechos que han caracterizado a la burocracia mexicana como lentas, ineficientes, obsoletas y ambiguas. El tomador de decisiones tiende a mostrar su limitado conocimiento del funcionamiento de la administración pública a partir del uso excesivo del instrumento de la centralización, de manera que se crea un bucle en su actuar, que difícilmente puede avanzar a la par de los retos de la globalización.

43

Es evidente que las nuevas tendencias de los instrumentos y modelos de gestión tardan en ser abordados por los aparatos burocráticos, en muchas ocasiones como consecuencia de las distintas realidades administrativas, presupuestales y organizacionales en las que operan las administraciones públicas, sin embargo, la estrategia de cuidado de los datos personales, además de la necesidad de consolidar acciones transversales entre los diferentes órdenes de gobierno, también debe considerar estrategias administrativas como la descentralización, desconcentración y centralización dependiendo de las circunstancias que lo amerite.

Los esquemas de buena gobernanza impulsan a que la acción pública sea un acto corresponsable para disminuir los delitos por el uso indebido de la información, pero el gobierno deberá crear el diseño institucional acorde para que primeramente la ciudadanía sepa que existe un organismo público diseñado especialmente para atender el problema. En segundo lugar, se debe impulsar la potencialización administrativa a partir del fortalecimiento de recursos humanos, presupuestarios y de infraestructura. Los organismos públicos con nuevas encomiendas no deben observarse como acciones secundarias por atender, sino que deben manifestarse como acciones prioritarias en el mismo ejercicio gubernamental. Considerar el modelo de gestión de acuerdo con las necesidades de los organismos públicos permite encaminar una mayor eficiencia y agilidad para crear políticas públicas, tomando en cuenta la diversidad de contextos y necesidades para disminuir los riesgos en la protección de datos.

Al articular una política de cuidado de los datos personales, mediante diversos modelos de gestión, se fortalece el equipamiento organizacional e incentiva la

coordinación y transversalidad entre diversos organismos públicos, lo que puede conducir a una mayor eficiencia en la protección de los datos. En lugar de depender únicamente de una autoridad centralizada, debe incentivarse un esquema colaborativo de la protección de datos, aprovechando la especialización de los organismos que atienden el tema.

III. Conclusión

Salvaguardar los datos personales como principio ético universal, fortalece el cuidado de la democracia mediante una corresponsabilidad compartida. Se tomaría en cuenta la normativa que involucra el tratamiento de datos para operar estrategias administrativas y mejorar la estrategia de gestión para proteger de manera efectiva la información de las personas en la era digital. Estos elementos se complementan entre sí para garantizar la privacidad, la integridad y el respeto por los derechos individuales, promoviendo así una sociedad más justa, transparente y democrática, en la que todos los ciudadanos puedan confiar en el manejo ético y responsable de su información personal.

El compromiso de la administración pública es fortalecer su desarrollo organizacional para legitimar la coordinación de estrategias entre órdenes de gobierno. Por otra parte, uno de los asuntos pendientes de la administración pública es su equipamiento administrativo para enfrentar las formas evolutivas de los problemas públicos. Si consideramos que el cuidado de manejo de datos es un tema que involucra a todos los organismos públicos, es importante crear una misma línea base de trabajo, bajo el entendimiento de la complejidad del asunto, así como de su equipamiento administrativo. Es necesario que este acompañamiento se genere desde aspectos tecnológicos y de capacitación del servicio público, de manera que el cuidado de la privacidad ciudadana y de la información personal, debe considerarse como parte del compromiso democrático, vigilando el uso de nuestra información bajo la perspectiva ciudadana. Esta orientación permitirá fortalecer nuestro marco jurídico, reconociéndola como hechos de alta vulnerabilidad en la que estamos expuestos en cualquier momento. La influencia capitalista en cuanto formas de transacciones económicas sustituye las garantías de la tranquilidad e integridad por condiciones de eficacia y eficiencia. El ritmo de vida acelerado de la sociedad expone la vulnerabilidad de la administración pública para controlar dichas situaciones por lo que debe fortalecerse su accionar correctivo por el bien de nuestra vida privada.

IV. Referencias

- ARENAS RAMIRO, Mónica, «Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades», *Hacia un nuevo derecho europeo de protección de datos*, Valencia, España, Tirant Lo Blanch, 2015, <https://dialnet.unirioja.es/servlet/articulo?codigo=5157591>.
- Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*. Última reforma 2024.
- COLMENAREJO FERNÁNDEZ, Rosa, *Una ética para Big Data. Introducción a la gestión ética de datos masivos*, Barcelona, Editorial UOC, 2017.
- D'ACQUISTO, Giuseppe, *et al.*, «Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics», *European Union Agency*

for Network and Information Security (ENISA), diciembre de 2015,
[arXiv:1512.06000](https://arxiv.org/abs/1512.06000)

- FERNÁNDEZ CONTE, León, «Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea», *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, 4 de mayo de 2016, pp. 35-50, <https://www.editorialreus.es/libros/9788429019360/capitulos/antecedentes-y-proceso-de-reforma-sobre-proteccion-de-datos-en-la-union-europea/>.
- GARRIGA DOMÍNGUEZ, Ana, «Nuevos retos para la protección de datos personales», *en la Era del Big Data y de la computación ubicua*, Madrid, España, Dykinson S. L., 2015.
- HERNÁN ORTIZ, Ana, *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, España, Dykinson S. L., 2022.
- HODGSON, Geoffrey, «¿Qué son las instituciones?», *Revista CS*, Colombia, num. 8, julio-diciembre de 2011, pp. 17-53.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares, México, 2010.
- Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados, México 2017.
- WARREN, Samuel y BRANDEIS, Louis, «The Right to Privacy», *The Harvard Law Review*, Boston, Harvard University, núm. 4, 1980. pp. 180.