

Artículo

Del consentimiento al control: Evolución de la privacidad en la sociedad digital

Bolívar Aguirre^{1*}, Delmy Galdámez², Marcos Martínez³

Citation: Aguirre, B., Galdámez, D. & Martínez, M. (2025). Del consentimiento al control: Evolución de la privacidad en la sociedad digital. Proceedings of the 2025 Academy of Latin American Business and Sustainability Studies (ALBUS), San Miguel, El Salvador.

<https://doi.org/10.70469/ALBUS.07>



Copyright: © with the authors. This Open Access article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0).

1 Universidad Evangélica de El Salvador, El Salvador, bolivar.aguirre@uees.edu.sv
2 Universidad Evangélica de El Salvador, El Salvador, delmy.galdamez@uees.edu.sv
3 Universidad Evangélica de El Salvador, El Salvador, decanato.ccjj@uees.edu.sv

Resumen: El artículo recoge el análisis sobre la evolución del consentimiento informado en el contexto de la protección de datos personales. Se desarrolla a partir de un abordaje cualitativo de tipo documental, en el que se revisan fuentes secundarias que permiten comprender, interpretar y contextualizar el fenómeno estudiado. Inicialmente se hace la búsqueda de la información, posteriormente se organiza y sistematiza, finalizando con la interpretación crítica a partir de los hallazgos significativos. Este diseño metodológico permite identificar diferentes fases en el proceso evolutivo del consentimiento, iniciando por el concepto de privacidad y el reconocimiento de este como derecho fundamental; luego, el cambio en la representación del consentimiento en contextos diferentes; la necesidad de estructuras efectivas para el uso de bienes o servicios digitales; el conocimiento de los usuarios para tener el poder de controlar el uso de sus datos y los retos que junto a la inteligencia artificial se presentan en la sociedad digital. El abordaje deja en evidencia que se requiere un ajuste del modelo de consentimiento significativo, dinámico y contextualizado, en el marco de un ecosistema normativo, técnico y ético que acorte las brechas entre usuarios y los creadores de bienes o servicios digitales.

Palabras clave: Consentimiento, privacidad, control, derecho fundamental, sociedad digital.

1. Introducción

En la era de la sociedad digital, marcada por la hiperconectividad, la automatización y la creciente dependencia de los datos personales como recurso estratégico, el derecho a la privacidad ha experimentado una evolución sustantiva. Lo que antes se entendía como un ámbito reservado a la intimidad personal ha evolucionado, en el contexto de la sociedad digital, a un derecho fundamental: la autodeterminación informativa. Este principio reconoce que cada individuo debe tener el control sobre cómo, cuándo y para qué se utiliza su información personal. En este marco, el consentimiento informado se posiciona como una pieza clave del andamiaje jurídico, ya que actúa como el mecanismo mediante el cual las personas autorizan —o niegan— el tratamiento de sus datos, conforme a sus propias decisiones y voluntad.

No obstante, en contextos dominados por algoritmos, modelos predictivos y procesos de toma de decisiones automatizados, la concepción tradicional del consentimiento se encuentra en crisis. Esta herramienta jurídica enfrenta serias tensiones debido a desequilibrios estructurales entre usuarios y grandes plataformas digitales, así como a la proliferación de interfaces opacas y prácticas intrusivas que debilitan la autonomía de las personas. Como señala González Fuster (2022), en muchos casos el consentimiento ha dejado de representar una decisión libre e informada para convertirse en una formalidad que respalda esquemas económicos basados en la recolección intensiva de datos personales.

Partiendo de esta problemática, el presente artículo explora la evolución teórica, normativa y doctrinal del consentimiento informado, poniendo énfasis en su tránsito de una exigencia meramente formal a una manifestación efectiva del derecho al control sobre los propios datos. Se aborda el tránsito desde la noción

tradicional hacia un modelo más robusto, centrado en el empoderamiento de los titulares, el diseño ético de sistemas digitales (Privacy by Design) y el reconocimiento del consentimiento como parte de un sistema más amplio de garantías, como los derechos ARCO-POL.

Finalmente, se realiza una vinculación con el contexto salvadoreño, donde la reciente entrada en vigencia de la Ley de Protección de Datos Personales (LPDP) y la Ley de Ciberseguridad y Seguridad de la Información (LCI), ambas en 2024, representan un avance significativo hacia la consolidación de un régimen jurídico de protección de datos basado en estándares internacionales. Este estudio sienta así las bases para un análisis posterior sobre el grado de armonización normativa entre el marco nacional e instrumentos jurídicos internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

2. Revisión de literatura

2.1. La privacidad como derecho fundamental

La privacidad, como derecho subjetivo, ha sido históricamente concebida como una garantía frente a injerencias externas en la esfera personal. En sus orígenes, se vinculaba al derecho a “estar solo”, como lo formularon Warren y Brandeis (1890) en el célebre artículo publicado en la Harvard Law Review. En el contexto del siglo XXI, la privacidad ha dejado de entenderse únicamente como un refugio frente a la intromisión para convertirse en el derecho al control sobre los datos personales y, por extensión, sobre la propia identidad digital. Desde esta perspectiva, Solove (2008) propone una clasificación de los daños a la privacidad que va más allá de la invasión directa e incorpora fenómenos como la vigilancia sistemática, la recolección desproporcionada y el uso inadecuado de la información. Según este autor, la privacidad no es un estado pasivo que se posee, sino un proceso activo que exige capacidad de decisión y de gestión sobre la información que se comparte.

El reconocimiento internacional de la privacidad como derecho fundamental se ha consolidado mediante instrumentos clave, como el artículo 8 del Convenio Europeo de Derechos Humanos y el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea. Ambos vinculan la protección de datos con el respeto a la dignidad humana y al libre desarrollo de la personalidad. Bygrave (2014) destaca que este marco normativo europeo ha sido determinante para consolidar un modelo de gobernanza global basado en la centralidad de los derechos individuales.

A esta evolución se suma la doctrina de la autodeterminación informativa, establecida por el Tribunal Constitucional Federal Alemán en 1983 en el emblemático caso del “Censo Federal”. Dicha jurisprudencia sostuvo que cada individuo debe poder decidir quién accede, trata o comunica sus datos personales, principio que se ha incorporado en diversas legislaciones y que ha servido de fundamento para los actuales estándares de finalidad, proporcionalidad, minimización de datos y transparencia en el tratamiento de la información.

2.2. El consentimiento informado: definición y transformaciones

En el marco de la protección de datos personales, el consentimiento ha sido históricamente reconocido como la principal base jurídica que legitima el tratamiento de la información. Esta figura jurídica actúa como expresión de la voluntad del titular y constituye una manifestación de control sobre sus propios datos. Según lo establecido en el artículo 6 del Reglamento General de Protección de Datos (RGPD), para que el consentimiento sea válido, debe reunir condiciones específicas: debe otorgarse de manera libre, ser específico en cuanto a su finalidad, estar claramente informado y no dejar lugar a ambigüedades, es decir, inequívoco. Esto significa que el titular debe tener la opción real de aceptar o rechazar el tratamiento sin consecuencias negativas, comprender claramente la finalidad y manifestar su voluntad de forma explícita.

Sin embargo, la práctica ha demostrado que el consentimiento puede ser fácilmente desvirtuado mediante prácticas como los “patrones oscuros” (dark patterns), interfaces que inducen al usuario a aceptar condiciones de manera poco ética. En esa misma línea, el Comité Europeo de Protección de Datos (2020), conocido por sus siglas en inglés EDPB, ha emitido orientaciones específicas para fortalecer los requisitos del consentimiento, con el objetivo de evitar prácticas engañosas que lo desvirtúen. Como advierten De Hert y Papakonstantinou (2012), en el entorno de la economía digital el consentimiento ha sido despojado de su fuerza jurídica real: los usuarios, muchas veces, aceptan condiciones extensas sin leerlas, motivados más por la necesidad de utilizar un servicio que por una comprensión real del tratamiento de sus datos. Este fenómeno revela la urgencia de redefinir el consentimiento desde un enfoque más robusto, en el que no solo se otorgue una autorización inicial, sino que también se garantice el ejercicio efectivo de derechos como el acceso, la cancelación o la oposición.

En este nuevo paradigma, el consentimiento ya no es simplemente un acto aislado al inicio del tratamiento, sino que forma parte de un ecosistema de gobernanza de datos personales basado en la responsabilidad y el control continuos. En este sentido, el enfoque de Privacy by Design, tal como lo explican Kool et al. (2010), plantea una solución estructural al incorporar la protección de la privacidad desde la concepción misma de los sistemas tecnológicos, y no como una corrección posterior o secundaria.

3.3. *El consentimiento informado en la era digital: implicaciones tecnológicas y jurídicas*

La digitalización ha modificado profundamente los mecanismos mediante los cuales se recopilan, procesan y comparten los datos personales, lo que obliga a replantear el consentimiento informado no solo como una base legal, sino también como una manifestación sustantiva del derecho a la privacidad. Mientras que en contextos físicos el consentimiento solía implicar una expresión explícita y voluntaria, frecuentemente firmada o otorgada presencialmente, en el entorno digital estas garantías se ven difuminadas. Hoy, es común que el consentimiento se manifieste mediante la selección de casillas premarcadas, la aceptación de textos legales extensos o la navegación por configuraciones predeterminadas que no siempre resultan claras ni comprensibles para el usuario promedio.

Ante esta realidad, Bélissent (2010) advierte que la automatización de los procesos asociados al tratamiento de datos impone una revisión crítica sobre la efectividad del consentimiento: ¿podemos considerarlo genuino cuando se integra en flujos digitales complejos o cuando se condiciona el acceso a servicios esenciales? Esta problemática ha sido ampliamente discutida en Europa y ha impulsado la consolidación del principio de Privacy by Design, que exige incorporar medidas de protección de datos desde el diseño inicial de cualquier sistema y no relegarlas a un momento posterior, como tradicionalmente se hacía.

En este contexto, el consentimiento informado debe entenderse en clave multidimensional. No basta con que el titular acepte voluntariamente el tratamiento de sus datos; también deben existir garantías estructurales que respalden esa decisión, tales como configuraciones predeterminadas de protección, interfaces comprensibles y mecanismos efectivos para revocar el consentimiento en cualquier momento. Tal como señala Bygrave (2014), la doctrina coincide en que la mera formalización del consentimiento pierde sentido si el entorno digital propicia prácticas de tratamiento desmedidas o poco transparentes.

Los desafíos se acentúan aún más en sistemas que emplean inteligencia artificial o tecnologías de big data, donde los datos recolectados pueden ser reutilizados para fines distintos a los inicialmente informados, o bien combinados con otros conjuntos de datos para generar perfiles automatizados. Esta situación tensiona el principio de finalidad y requiere salvaguardas adicionales, como la información continua, el control activo por parte del titular y un derecho efectivo de oposición (González Fuster, 2014).

En definitiva, el consentimiento informado en entornos digitales no puede concebirse como una mera cláusula contractual. Su verdadero valor reside en que constituye una pieza estructural que articula la protección de derechos fundamentales con las responsabilidades técnicas, jurídicas y éticas de quienes diseñan y administran los sistemas de tratamiento de datos.

2.4. *El consentimiento como instrumento de autodeterminación informativa*

El consentimiento informado ha sido tradicionalmente entendido como una expresión individual y voluntaria que autoriza el tratamiento de datos personales. No obstante, en el marco de la sociedad digital contemporánea, este concepto adquiere una dimensión más compleja al convertirse en una manifestación tangible del principio de autodeterminación informativa. Este principio reconoce el derecho de cada persona a decidir, de manera autónoma y consciente, cómo y para qué se utiliza su información personal, lo que lo convierte en una piedra angular de la protección de datos en entornos hipertecnologizados.

Su origen jurídico se remonta a la célebre sentencia del Tribunal Constitucional Federal Alemán sobre el Censo de Población de 1983, en la que se definió la autodeterminación informativa como el derecho de todo individuo a determinar por sí mismo la revelación y utilización de sus datos personales. Esta doctrina sentó un precedente fundamental al establecer que el consentimiento no es solo un acto formal que autoriza el tratamiento, sino también una herramienta para ejercer control y soberanía frente a estructuras de poder —estatales o privadas— que recolectan y procesan datos con fines diversos.

Sin embargo, este modelo se enfrenta hoy a desafíos estructurales. La brecha de poder y conocimiento entre quienes diseñan e implementan las tecnologías y los titulares de los datos se ha ampliado considerablemente. La complejidad de los sistemas algorítmicos, la opacidad de las plataformas digitales y las lógicas económicas basadas en la explotación masiva de datos generan un entorno en el que la autodeterminación informativa corre el riesgo de convertirse en una ficción si no se acompaña de mecanismos jurídicos y técnicos que refuercen la capacidad efectiva de decisión de los usuarios.

Según González Fuster (2014), esta tensión evidencia que el consentimiento ha sido instrumentalizado en muchos contextos como una herramienta de legitimación aparente, especialmente cuando se recopila de forma generalizada, sin posibilidad real de oposición, o cuando se presenta como condición para acceder a bienes o servicios digitales esenciales.

A ello se suma la crítica de Bygrave (2014), quien advierte que, si bien el consentimiento sigue siendo una base legal central, su efectividad está erosionada por la complejidad técnica de los tratamientos de datos, las

prácticas de perfilado automático y reutilización de información para fines no previsibles para el usuario. Esta situación compromete la genuina autodeterminación del titular de los datos, especialmente cuando no existen opciones claras ni mecanismos efectivos para el ejercicio de los derechos.

Desde el enfoque Privacy by Design, el consentimiento debe estar acompañado de garantías estructurales que permitan su ejercicio efectivo. Cavoukian (2011), creadora del enfoque, propone que las decisiones sobre el uso de los datos deben estar insertas en un diseño institucional que favorezca la transparencia, la rendición de cuentas y la posibilidad de revocar el consentimiento sin obstáculos. Esto implica diseñar sistemas en los que el consentimiento no sea un trámite formal, sino un proceso continuo de toma de decisiones e información, sostenido mediante medios técnicos como paneles de control personalizados, configuraciones predeterminadas respetuosas de la privacidad y avisos proactivos sobre cambios en el tratamiento.

Por su parte, el RGPD de la UE (2016/67) refuerza esta visión al establecer en su considerando 32 y artículo 4.11 que el consentimiento debe ser “libre, específico, informado e inequívoco” y que su manifestación debe constituir una clara acción afirmativa. Asimismo, impone a los responsables del tratamiento la carga probatoria (art. 7) y establece que el consentimiento no será válido si existe un desequilibrio de poder entre las partes.

En este sentido, puede afirmarse que el consentimiento, como manifestación de autodeterminación informativa, no puede analizarse de forma aislada, sino que debe entenderse como parte de un ecosistema normativo, técnico y ético que garantice la dignidad de la persona en la era digital. La autodeterminación no es solo un derecho pasivo a ser informado, sino también un poder activo para controlar el destino de la propia información.

La consolidación del consentimiento como un mecanismo genuino de autodeterminación informativa exige, necesariamente, reconocer que existen contextos en los que dicha autodeterminación puede verse comprometida. Entornos como el educativo, el laboral o el sanitario, caracterizados por relaciones de poder o dependencia, pueden reducir significativamente la libertad real de elección, convirtiendo el consentimiento en una formalidad más que en una decisión autónoma y voluntaria.

En este sentido, la literatura especializada ha advertido sobre la necesidad de evaluar no solo los aspectos jurídicos del consentimiento, sino también sus implicaciones éticas y sociales. Mantelero (2014), por ejemplo, sugiere la adopción de marcos de evaluación que permitan determinar si el consentimiento obtenido es realmente válido o si se da en condiciones estructuralmente limitantes. Para este autor, es fundamental avanzar hacia modelos más integrales de gobernanza algorítmica, donde se priorice la responsabilidad proactiva de quienes desarrollan y operan tecnologías, así como la exigencia de justificación algorítmica, es decir, la obligación de explicar y fundamentar de forma comprensible las decisiones de los sistemas automatizados.

Desde esta perspectiva, el consentimiento no puede tratarse como un elemento aislado del ecosistema digital, sino como parte de un entramado más amplio de garantías que aseguren el respeto a la dignidad, la igualdad y la autonomía de los individuos, especialmente en situaciones de vulnerabilidad.

2.5. Evolución del consentimiento en el entorno digital: del formalismo al consentimiento significativo

La transición desde una sociedad analógica a un ecosistema digital complejo ha transformado profundamente el rol del consentimiento en el marco de la protección de datos personales. Lo que antes se concebía como una exigencia meramente formal —frecuentemente reducida a la aceptación de condiciones contractuales extensas e ininteligibles— ha evolucionado hacia un instrumento clave para salvaguardar los derechos fundamentales de las personas, particularmente en contextos marcados por la vigilancia algorítmica, el desarrollo de sistemas de inteligencia artificial y el procesamiento masivo de datos (big data).

Esta transformación no ha sido casual ni automática. Ha estado acompañada de un progresivo fortalecimiento de los marcos regulatorios, así como del impulso crítico de la academia, que ha puesto en evidencia los riesgos asociados a la opacidad tecnológica y a la pérdida de control individual sobre la información personal. A su vez, los rápidos avances en las capacidades de procesamiento de datos han desafiado los esquemas tradicionales de control, obligando a repensar el consentimiento no solo como un acto aislado, sino como parte de una arquitectura más amplia de garantías sustantivas y procesales que favorezcan la autodeterminación informativa en escenarios digitales altamente tecnificados.

Tal como advierte Tzanou (2017), en el entorno digital contemporáneo, el consentimiento ha sido progresivamente vaciado de su esencia protectora debido a la práctica habitual de presentar políticas de privacidad excesivamente extensas, técnicas o ambiguas. Este tipo de documentación, lejos de empoderar al usuario, suele ser aceptado sin una lectura previa ni comprensiva, motivado más por la necesidad inmediata de utilizar un servicio que por una verdadera comprensión del alcance del tratamiento de sus datos. Esta práctica ha dado lugar al fenómeno conocido como “fatiga del consentimiento” (consent fatigue), que describe una automatización pasiva del acto de consentir, reduciéndolo a una formalidad carente de reflexión, lo que socava su rol como garantía efectiva de la autodeterminación informativa.

Numerosos enfoques doctrinales coinciden en señalar que el modelo tradicional del consentimiento, basado en la mera aceptación formal, resulta insuficiente ante los actuales tratamientos de datos, caracterizados por su complejidad, opacidad y automatización. En esta línea, Nissenbaum (2010) plantea la necesidad de replantear el concepto de privacidad desde el principio de “integridad contextual” (contextual integrity), que exige el respeto a las normas sociales que regulan el flujo de información en contextos específicos. Así entendido, el consentimiento no se limita a la autorización de finalidades y medios, sino que solo puede considerarse legítimo si el titular comprende plenamente las implicaciones situadas de dicho tratamiento: su posible reutilización, la generación de perfiles, la toma de decisiones automatizadas o los impactos futuros en otros entornos sociales. Este enfoque propone, por tanto, una concepción más rica y contextualizada del consentimiento que responda a la complejidad de las interacciones digitales contemporáneas.

Frente a los desafíos del consentimiento formalista, el enfoque actual privilegia el concepto de consentimiento significativo, que exige condiciones más robustas en cuanto a claridad, accesibilidad y centración en la experiencia del usuario. Esta perspectiva ha sido respaldada por instituciones como la Agencia Española de Protección de Datos, que en su guía de 2021 destaca la importancia de emplear mecanismos dinámicos que favorezcan la comprensión efectiva por parte del titular. Entre estos mecanismos se incluyen la presentación segmentada de las finalidades del tratamiento, interfaces de gestión de preferencias, explicaciones contextuales en lenguaje sencillo y opciones visibles para tomar decisiones en tiempo real. Asimismo, este modelo requiere que la revocación del consentimiento sea posible en cualquier momento, sin generar fricciones técnicas ni consecuencias negativas para quien la ejerce. En suma, el consentimiento significativo no solo habilita el tratamiento de datos, sino que también empodera a la persona como sujeto activo en la gobernanza de su información.

En coherencia con los estándares emergentes sobre protección de datos, la Directiva (UE) 2019/770 relativa a los contratos de suministro de contenidos y servicios digitales establece que el consentimiento debe ser otorgado de manera libre, específica e informada y pierde su validez si se condiciona el acceso a bienes o servicios cuya prestación no lo requiere. Este principio busca evitar prácticas coercitivas o engañosas que desdibujen la autonomía del titular. Esta visión ha sido adoptada progresivamente por diversos marcos normativos, entre ellos la Ley para la Protección de Datos Personales de El Salvador (LPDP, 2024), que, en su artículo 27, recoge de forma explícita los elementos esenciales del consentimiento válido: libre, específico, informado, expreso e individualizado. De este modo, la LPDP no solo alinea al país con estándares internacionales, sino que también delimita con claridad las condiciones bajo las cuales el consentimiento puede ser legalmente considerado una expresión auténtica de la voluntad del titular.

En escenarios donde se aplican tecnologías complejas como los sistemas de inteligencia artificial orientados al reconocimiento emocional, el consentimiento significativo requiere un enfoque más amplio que contemple no solo la autorización explícita del titular, sino también los posibles efectos colaterales del tratamiento. Entre estos riesgos destacan la discriminación algorítmica, los sesgos sistemáticos en la interpretación emocional y la generación de inferencias psicológicas sin fundamento ni consentimiento adicional. Frente a estas problemáticas, Wachter y Mittelstadt (2019) sostienen que el consentimiento debe complementarse con salvaguardas estructurales, tales como evaluaciones éticas previas, auditorías sobre el funcionamiento de los algoritmos y transparencia técnica en el diseño y funcionamiento de los sistemas. Estas medidas no sustituyen el consentimiento, sino que lo robustecen, garantizando una protección efectiva en entornos donde las decisiones automatizadas pueden tener repercusiones sustanciales sobre la autonomía y dignidad de las personas.

En síntesis, el desarrollo normativo y doctrinal del consentimiento ha desplazado su énfasis de una visión meramente formal a una comprensión más sustantiva y centrada en el usuario. Se no se trata de obtener una aceptación rutinaria, sino de garantizar que las personas comprendan plenamente el alcance y las implicaciones del tratamiento de sus datos. Esta evolución es clave para restablecer el equilibrio entre quienes administran los sistemas tecnológicos y quienes están sujetos a sus efectos, y constituye un componente esencial para abordar con responsabilidad los desafíos jurídicos y éticos que plantea la sociedad digital actual.

2.6. El consentimiento en el contexto de la IA: retos actuales y proyecciones futuras

La expansión de la inteligencia artificial (IA) en sectores clave como la salud, la educación, el mundo laboral y los servicios financieros ha introducido cambios profundos en la forma en que se recopilan y procesan los datos personales. La creciente sofisticación de los algoritmos, sumada a su capacidad para extraer información altamente sensible a partir de fuentes que, en apariencia, no revelan datos personales, plantea serios desafíos al modelo tradicional de consentimiento. Este nuevo escenario obliga a replantear las bases legales del consentimiento informado, exigiendo que se conciba no solo como un trámite formal, sino también como una garantía sustantiva del derecho a decidir sobre la propia información.

En escenarios donde los sistemas de inteligencia artificial operan de forma autónoma o con mínima supervisión humana, garantizar que los titulares comprendan plenamente el alcance y las implicaciones del

tratamiento de sus datos resulta complejo. Como advierten Floridi et al. (2018), estos sistemas pueden tomar decisiones de manera opaca, tanto para los usuarios como para los propios desarrolladores. Esta falta de transparencia técnica crea una brecha cognitiva significativa, que pone en entredicho la validez del consentimiento otorgado, especialmente cuando se trata de tecnologías capaces de inferir estados mentales —como el reconocimiento emocional— sin que exista participación activa o conciencia del sujeto respecto a dicha actividad.

Desde la perspectiva jurídica, tanto el Reglamento General de Protección de Datos (RGPD) como las recomendaciones formuladas por el Consejo de Europa y la Organización para la Cooperación y el Desarrollo Económico (OCDE) subrayan que, en contextos en los que intervienen tecnologías automatizadas, el consentimiento debe cumplir con requisitos estrictos: debe ser explícito, informado y revocable. Además, se exige que los responsables del tratamiento implementen mecanismos técnicos y organizativos que garanticen el ejercicio efectivo de este consentimiento en cualquier momento, evitando que se convierta en una mera formalidad vacía de contenido. La necesidad de implementar el principio de transparencia algorítmica —esto es, permitir que las personas comprendan cómo sus datos son procesados por un sistema de IA— se ha convertido en un imperativo ético y jurídico (Wachter, Mittelstadt & Floridi, 2017).

El principio de Privacy by Design, consagrado en el artículo 25 del Reglamento General de Protección de Datos (RGPD), cobra especial relevancia en el ámbito de la inteligencia artificial. Esta perspectiva exige que los sistemas tecnológicos incorporen, desde su diseño inicial, salvaguardas estructurales que garanticen la protección de los datos personales. En este marco, el consentimiento debe concebirse no como un acto aislado previo al tratamiento, sino como una dimensión continua, capaz de adaptarse al uso progresivo del sistema. En esa línea, Mantelero (2018) propone un modelo de consentimiento adaptativo mediante el cual los titulares pueden modificar sus decisiones y preferencias a medida que interactúan con las funcionalidades del sistema, lo que favorece un control real y evolutivo sobre su información personal.

En el marco normativo salvadoreño, la Ley para la Protección de Datos Personales (LPDP, 2024) establece el consentimiento informado como requisito esencial para el tratamiento de datos personales, en particular cuando se trata de información sensible. Sin embargo, frente a los retos que plantea el uso de tecnologías basadas en inteligencia artificial, esta garantía legal resulta insuficiente si no se complementa con mecanismos institucionales más robustos. En este sentido, la implementación de auditorías algorítmicas, procesos de evaluación de impacto en la protección de datos y supervisión ética permanente se vuelve imprescindible. Aunque estos elementos aún se encuentran en una fase incipiente en el ordenamiento jurídico nacional, su desarrollo será clave para armonizar la normativa salvadoreña con los estándares internacionales en materia de derechos digitales y de gobernanza algorítmica.

De igual forma, la Ley de Ciberseguridad y Seguridad de la Información (LCSI, 2024) complementa el marco de protección de datos al establecer, en sus artículos 6 y 8, una serie de obligaciones orientadas a fortalecer la seguridad digital. Aunque esta normativa no aborda explícitamente el consentimiento informado, sí impone el cumplimiento de estándares internacionales y la adopción de buenas prácticas en el desarrollo y uso de tecnologías emergentes, incluida la inteligencia artificial. Estas disposiciones refuerzan indirectamente la validez y eficacia del consentimiento, al exigir que los sistemas tecnológicos incorporen principios de ética digital, gestión de riesgos, auditoría y cooperación con organismos especializados. En conjunto, tales medidas buscan asegurar un entorno de confianza en el que el consentimiento no solo se otorgue, sino también se respete y proteja mediante salvaguardas técnicas y organizativas.

En consecuencia, uno de los principales retos para el futuro del consentimiento informado en contextos de inteligencia artificial radica en su adecuada implementación técnica en entornos dinámicos, con autonomía algorítmica y descentralización. Para afrontar este desafío, resulta indispensable diseñar mecanismos comprensibles y accesibles que permitan al usuario revisar, modificar o revocar su consentimiento en tiempo real, sin comprometer la operatividad del sistema. Esta evolución no solo responde a exigencias técnicas, sino también a un cambio de paradigma ético que sitúa al ser humano en el centro de los procesos tecnológicos. En esta línea, autores como Cath (2018) proponen una ética digital fundamentada en el principio de agencia informacional, entendida como la capacidad efectiva de los individuos para tomar decisiones conscientes y controladas sobre el uso de su información personal.

De este modo, el consentimiento informado deja de ser únicamente un requisito jurídico para convertirse en un componente esencial del diseño ético y técnico de sistemas algorítmicos responsables. Su correcta implementación no solo legitima el tratamiento de datos, sino que también actúa como un contrapeso frente al poder de las tecnologías emergentes, al asegurar que los derechos fundamentales permanezcan en el centro de la innovación. Esta perspectiva exige el desarrollo de marcos normativos y arquitecturas digitales interoperables que permitan armonizar la eficiencia de los sistemas de inteligencia artificial con los principios de dignidad humana, autonomía individual y control efectivo sobre los datos personales.

3. Materiales y metodología

La investigación se desarrolla desde un enfoque cualitativo de tipo documental, orientado al análisis y la sistematización de información proveniente de fuentes secundarias. Este enfoque permite comprender, interpretar y contextualizar el fenómeno de estudio a partir de los aportes teóricos disponibles en el marco de la temática estudiada. Tiene un diseño metodológico que implica 3 fases.

La fase 1 consistió en la recolección de la información documental. En esa fase se realizó una búsqueda exhaustiva de fuentes bibliográficas en bases de datos que cumplieran con criterios de inclusión, como: relevantes al objeto de estudio, información verídica de fuentes confiables. No se consideran documentos o fuentes bibliográficas que no contengan respaldo jurídico o cuya procedencia no pueda verificarse.

La fase 2 consiste en la organización y sistematización de la información, la cual se realizó mediante una matriz de análisis documental, en la que se clasifican las fuentes para identificar a los autores, el tipo de documentos y los principales hallazgos. En esta etapa se identifican patrones teóricos vacíos, tendencias o cambios en el fenómeno de estudio. Finalmente, la fase 3 consistió en el análisis e interpretación de fuentes secundarias. Se aplicó un análisis de contenido temático para identificar categorías de estudio relacionadas con el problema de investigación. Posteriormente, se realizó la interpretación de forma crítica, contrastando autores, posturas o elementos teóricos, destacando las principales contribuciones para comprender el fenómeno.

Para garantizar la validez y la confiabilidad del proceso, se desarrolló una triangulación de fuentes, es decir, se compararon distintos autores, tipos de documentos y criterios de calidad para determinar la pertinencia, la actualidad, la autoridad y la relevancia de las fuentes.

4. Resultados

En el proceso de evolución conceptual y normativa del consentimiento informado en el ámbito de la protección de datos personales, se destaca su transformación de una autorización formal en un instrumento clave de autodeterminación informativa. En este proceso de evolución se pueden identificar cinco etapas interrelacionadas:

Etapas 1: El reconocimiento de la privacidad como derecho fundamental de las personas: en esta etapa se establece que la privacidad ha pasado de ser entendida como el derecho a estar solo a convertirse en el derecho a controlar los datos personales, con implicaciones directas sobre la identidad digital, que actualmente es indispensable en la dinámica de la sociedad.

Etapas 2. Reformulación del consentimiento: es notable que el consentimiento, aunque históricamente se ha considerado una base jurídica para autorizar el tratamiento de información personal. En la actualidad se ve debilitado por prácticas manipulativas, como los denominados patrones oscuros, y por la sobrecarga informativa, hasta el punto de llevarlo a un escenario en la esfera digital, donde los usuarios responden a contextos que difieren del deber ser: libre, específico, informado e inequívoco.

Etapas 3. Impacto de la digitalización: la automatización y complejidad de los sistemas digitales han desafiado la validez del consentimiento tradicional; esto conlleva la exigencia de nuevas garantías estructurales como la transparencia, la revocabilidad y la configuración predeterminada de privacidad, donde los usuarios no estén en riesgo de ser víctimas de diseños no controlados y de tratamiento excesivo de datos personales.

Etapas 4. Consentimiento como manifestación de autodeterminación informativa: se presta especial atención a profundizar en la idea de que el consentimiento debe ser una expresión activa del control sobre los datos, especialmente en contextos de vulnerabilidad o desequilibrio de poder. Con el fin de que cada persona tenga pleno poder para decidir sobre el uso de sus datos.

Etapas 5. Retos de la inteligencia artificial - IA: los desafíos específicos en entornos algorítmicos, donde la opacidad y la inferencia de datos sensibles requieren un consentimiento dinámico, adaptativo y respaldado por mecanismos técnicos y éticos, evidencian las brechas que existen en lo relativo al conocimiento de los usuarios sobre el funcionamiento de los algoritmos y que no respondan únicamente a un comportamiento mecánico motivado por la necesidad del uso de éstos.

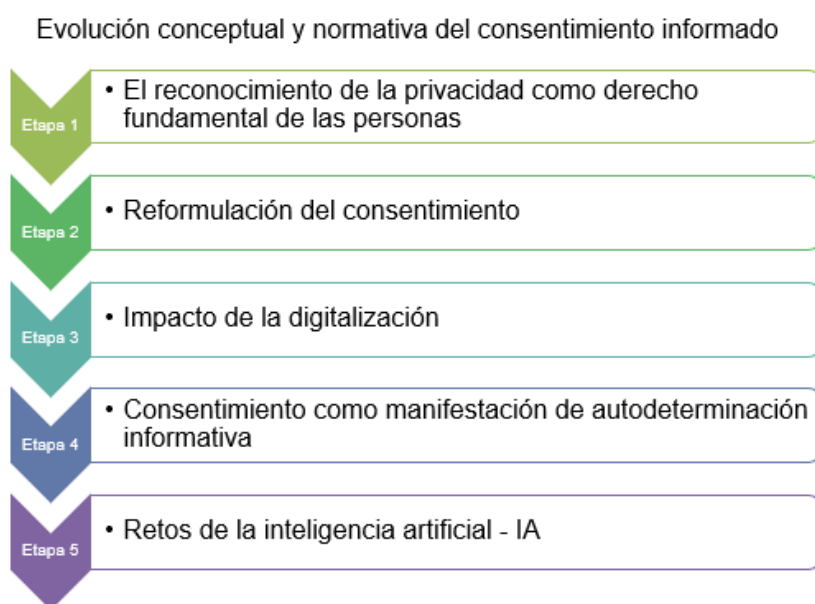


Figura 1. Ilustración 1. Evolución del consentimiento informado. Elaboración propia, 2025.

En el contexto de la sociedad digital, el concepto de privacidad supera la idea de intromisión y conlleva una serie de implicaciones respecto del control de la información personal. Por tal razón, es evidente que el consentimiento debe representar la manifestación libre e informada, donde el titular de los datos tenga el conocimiento de cada una de las implicaciones y claridad de lo que puede o no revocar del mismo, con el fin de garantizar que el consentimiento este fundamentado en el libre ejercicio de su derecho a decidir sobre el uso de sus datos, más allá de la necesidad de cumplir un requisito para acceder a bienes o servicios digitales. En tal sentido, desde el diseño se debe actuar con ética y considerar la existencia de mecanismos efectivos para la protección de datos y la garantía de los derechos, tal como se han concebido en cada uno de los instrumentos normativos existentes a nivel nacional o internacional.

Cabe señalar que Solove y Bygrave sostienen que la privacidad debe entenderse como un proceso activo de gestión de la información, mientras que otros, como Nissenbaum y Wachter, proponen enfoques contextuales y éticos para abordar los desafíos de la IA. Sin embargo, al margen del enfoque de cada uno de estos autores, se evidencia el respaldo de la idea central de este escrito, evidenciar las exigencias del contexto para generar modelos o estructuras respaldadas por los marcos normativos que son referentes a nivel internacional, y la adopción de normas de aplicación nacional que reduzcan las asimetrías de poder en torno al control que tienen los usuarios y los creadores de bienes o servicios digitales.

Sin embargo, existen tensiones, ya que algunos críticos señalan que el consentimiento, incluso reforzado, puede verse limitado ante la complejidad técnica y las diferencias de poder. A partir de lo señalado, se evidencia la necesidad de modelos complementarios, como la responsabilidad proactiva, la justificación algorítmica o la evaluación ética, los cuales representan retos significativos para la denominada sociedad digital.

Por tanto, se evidencia que el consentimiento ha dejado de ser un requisito legal para convertirse en un componente fundamental de la gobernanza digital. Además, se identifican límites del consentimiento tradicional y se deja expuesto que se está evolucionando hacia la creación de mecanismos con estructuras más efectivas. Finalmente, con la IA queda clara la necesidad de realizar ajustes y adaptar el consentimiento mediante herramientas técnicas y marcos normativos robustos.

5. Conclusiones

El consentimiento informado ha evolucionado desde una concepción de formalidad jurídica hasta un instrumento de empoderamiento de los ciudadanos en la era digital. Esta transformación es congruente con estudios previos que proponen una protección de datos cuyo enfoque esté en los derechos humanos. También, al comparar lo contemplado en distintos marcos normativos, se reconoce una visión integral en la que se vinculan el consentimiento, la dignidad humana y la autodeterminación.

El consentimiento significativo no puede depender únicamente de la voluntad de los individuos, sino que debe contar con el respaldo de estructuras técnicas, jurídicas y éticas que garanticen su efectividad.

En contextos de IA, el consentimiento debe dar respuestas a las dinámicas y contextos en los que se solicite, esto implica rediseñar las interfaces y los sistemas de toma de decisiones que respondan a cada una de esas exigencias.

Referencias:

- Bélissent, J. (2010). Getting clever about smart cities: New opportunities require new business models. Forrester Research. <https://www.forrester.com/report/Getting-Clever-About-Smart-Cities-New-Opportunities-Require-New-Business-Models/RES56701>
- Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press. Reino Unido. <https://global.oup.com/academic/product/data-privacy-law-9780199675555>
- Cath, C. (2018). Gobernanza de la inteligencia artificial: oportunidades y desafíos éticos, legales y técnicos. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180080. <https://doi.org/10.1098/rsta.2018.0080>
- Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. Canadá. https://www.datatilsynet.no/globalassets/global/bilder/rettigheter-og-plikter/innebygd-personvern/7foundationalprinciples_annocavoukian2.pdf
- De Hert, P., & Papakonstantinou, V. (2012). El Reglamento de protección de datos propuesto que sustituye a la Directiva 95/46/CE: Un sistema sólido para la protección de las personas. *Computer Law & Security Review*, 28(2), 130-142. <https://doi.org/10.1016/j.clsr.2012.01.006>
- De Santa María, P. A. S. (2008). La Carta de los Derechos Fundamentales de la Unión Europea en la práctica española. *Revista de derecho de la Unión Europea*, (15), 233-255. <https://revistas.uned.es/index.php/REDUE/article/view/12539>
- Diario Oficial de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People: un marco ético para una buena sociedad de IA: oportunidades, riesgos, principios y recomendaciones. *Minds and Machines*, 28(4), 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
- González Fuster, G. (2021). Study on the essence of the fundamental rights to privacy and to protection of personal data. European Parliament. https://www.edps.europa.eu/system/files/2023-11/edps-vub-study_on_the_essence_of_fundamental_rights_to_privacy_and_to_protection_of_personal_data_en.pdf
- Herdero Campo, M. T. (2019). Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales [DOUE L 136/1, de 22-V-2019]. *AIS: Ars Iuris Salmanticensis*, 7(2), 263-265. <https://revistas.usal.es/cuatro/index.php/ais/article/view/22499>
- Higueras, M. H. (1983). La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983. Documentación administrativa. <https://dialnet.unirioja.es/servlet/articulo?codigo=220507>
- Mantelero, A. (2014). El futuro de la protección de datos de los consumidores en la UE: Replanteamiento del paradigma de «notificación y consentimiento» en la nueva era del análisis predictivo. *Computer Law & Security Review*, 30(6), 643-660. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529245
- Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press. Estados Unidos. ISBN: 9780804752367 <https://www.sup.org/books/law/privacy-context>
- OECD. (2018). Guía de la OCDE de Devida Diligencia para una Conducta Empresarial Responsable. OECD Publishing. Francia. https://www.oecd.org/es/publications/guia-de-la-ocde-de-devida-diligencia-para-una-conducta-empresarial-responsable_14922561-es.html
- Solove, D. J. (2010). Understanding privacy. Harvard University Press. Estados Unidos. ISBN 9780674035072 <https://www.hup.harvard.edu/catalog.php?isbn=9780674035072>
- Tribunal Europeo de Derechos Humanos. (1953). Convenio europeo de derechos humanos. https://www.echr.coe.int/Documents/Convention_SPA.pdf
- Tzanou, M. (2017). The fundamental right to data protection: Normative value in the context of counter-terrorism surveillance (Vol. 71). Bloomsbury Publishing. Reino Unido. <https://www.bloomsbury.com/uk/search/?q=The%20fundamental%20right%20to%20data%20protection%3A%20Normative%20value%20in%20the%20context%20of%20counter-terrorism%20surveillance%20>
- Van Lieshout, M., Kool, L., van Schoonhoven, B., & de Jonge, M. (2011). Privacy by Design: an alternative to existing practice in safeguarding privacy. *info*, 13(6), 55-68.

https://www.researchgate.net/publication/242025627_Privacy_by_Design_An_alternative_to_existing_practice_in_safeguarding_privacy

Wachter, S., & Mittelstadt, B. (2019). El derecho a inferencias razonables: replanteando la legislación sobre protección de datos en la era del big data y la IA. *Columbia Business Law Review*, 2019(2), 494-620. <https://journals.library.columbia.edu/index.php/CBLR/article/view/3424>

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). IA transparente, explicable y responsable para la robótica. *Science Robotics*, 2(6), eaan6080. <https://ora.ox.ac.uk/objects/uuid:fd0a0307-dc89-488e-bdec-4a100d1f073e>