

PRÁCTICAS ABUSIVAS EN EL ECOSISTEMA DIGITAL: LA VULNERABILIDAD DEL CONSENTIMIENTO FRENTE A LAS PLATAFORMAS TRANSNACIONALES

INVESTIGACIÓN

PRACTICES IN THE DIGITAL ECOSYSTEM: THE VULNERABILITY OF CONSENT AGAINST TRANSNATIONAL PLATFORMS

RESUMEN

La presente investigación disecciona la vulnerabilidad estructural que oprime al consumidor mexicano frente al poderío de las plataformas digitales transnacionales. El objetivo rector consiste en describir las afectaciones jurídicas derivadas de una voraz asimetría informativa. Se evalúa con rigor la ineficacia material de los mecanismos de responsabilidad amparados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Para lograrlo, la metodología se cimentó en un diseño mixto explicativo secuencial (CUAL-cuan). Durante la primera fase, se realizó un análisis documental crítico-hermenéutico. La normativa nacional fue sometida a un escrutinio comparativo con los estándares garantistas del Reglamento General de Protección de Datos (RGPD) europeo. Posteriormente, la vertiente cuantitativa midió empíricamente tres barreras que debilitan el "consentimiento informado" en los contratos de adhesión digitales. Utilizando una muestra por conveniencia de los quince consorcios tecnológicos con mayor penetración comercial ($N=15$), se midieron la extensión absoluta, la fragmentación referencial y la legibilidad mediante el índice Flesch-Szigriszt. Los hallazgos revelaron un escenario insostenible. El usuario medio se enfrenta a volúmenes textuales que superan las cinco mil palabras, redactados con una sintaxis clasificada como "algo difícil" y plagados de hipervínculos dispersos. Tales estipulaciones vuelven materialmente imposible la asimilación humana de las cláusulas. El consentimiento expreso resulta una ficción desvirtuada por tácticas deliberadas de saturación cognitiva. A su vez, el esquema sancionatorio exhibe una nula fuerza disuasoria frente a entidades globales y opera bajo la desgastada lógica de la responsabilidad subjetiva. Como solución dogmática ante esta falla estructural innegable, la investigación concluye proponiendo la adopción imperativa de la responsabilidad civil objetiva por riesgo creado frente a la opacidad

GAYTÁN ROMÁN, José de Jesús

Facultad de Derecho, Universidad Autónoma de Coahuila. Torreón, Coahuila, México.

Correspondencia
gaytan-j@uadec.edu.mx
<https://orcid.org/0009-0002-4664-7996>
Fecha de recepción
11 de noviembre de 2025.
Fecha de aceptación
10 de junio de 2026.

algorítmica. Asimismo, se exige dotar de alcance extraterritorial a la jurisdicción mediante la integración del criterio de direccionamiento de servicios (*targeting*).

Palabras clave: protección de datos; asimetría de poder; prácticas abusivas; responsabilidad objetiva; contratos de adhesión.

ABSTRACT

This research dissects the structural vulnerability that oppresses the Mexican consumer in the face of the might of transnational digital platforms. The primary objective is to describe the legal impacts arising from a voracious informational asymmetry. The material ineffectiveness of the liability mechanisms protected by the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) is rigorously evaluated. To achieve this, the methodology was built upon an explanatory sequential mixed-methods design (QUAL-quant). During the initial phase, a critical-hermeneutical documentary analysis was executed. National regulations were subjected to comparative scrutiny against the protective standards of the European General Data Protection Regulation (GDPR). Subsequently, the quantitative strand empirically examined three barriers that undermine "informed consent" in digital adhesion contracts. Utilizing a convenience sample of the fifteen tech consortia with the highest commercial penetration (\$N=15\$), absolute length, referential fragmentation, and readability were measured through the application of the Flesch-Szigriszt index. The findings revealed an unsustainable scenario. The average user encounters text volumes exceeding five thousand words, drafted in a syntax classified as "somewhat difficult" and plagued by scattered hyperlinks. Such stipulations make human assimilation of the clauses materially impossible. Express consent turns out to be a fiction distorted by deliberate tactics of cognitive saturation. Furthermore, the sanctioning scheme exerts no deterrent effect on global entities, operating under the worn-out logic of subjective liability. As a dogmatic solution to this undeniable structural failure, the research concludes by proposing the imperative adoption of objective civil liability for created risk in the face of algorithmic opacity. Likewise, it requires extending the jurisdiction's extraterritorial scope by integrating the targeting criterion.

Keywords: *data protection; power asymmetry; abusive practices; objective liability; adhesion contracts.*

INTRODUCCIÓN

Para operar legalmente dentro de la jurisdicción nacional, la normatividad impone condiciones inexcusables. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares exige la manifestación de voluntad del titular (Cámara de Diputados del H. Congreso de la Unión, 2010). Lejos de imponerse coactivamente, las plataformas transnacionales condicionan la prestación de sus servicios a la aceptación de extensos términos y condiciones. Para poder usarse, dichas plataformas requieren que la persona marque una casilla de verificación, otorgando así su consentimiento expreso. Surgen, sin embargo, cuestionamientos imperativos sobre la validez y la eficacia material de este acto volitivo.

La doctrina contemporánea documenta ampliamente la "paradoja de la privacidad" (Barth & de Jong, 2017), un fenómeno empírico en el que los cibernautas exponen incesantemente su información a pesar de externar una profunda preocupación por su resguardo. Esta disonancia cognitiva no se debe exclusivamente a la negligencia individual del internauta. Emana de un diseño contractual rapaz. Los contratos de adhesión digitales desbordan deliberadamente las capacidades cognitivas del consumidor promedio, instituyendo cláusulas contractuales abusivas bajo la falaz apariencia de legalidad y transparencia. Frente a una saturación sistemática, el clic de aceptación se convierte en un ritual ciego, despojado de genuina libertad electiva.

El objetivo del presente trabajo radica en analizar la ineficacia fáctica del ordenamiento jurídico mexicano para responsabilizar a corporaciones transnacionales por prácticas abusivas en el tratamiento de datos personales. Se analizará la insuficiencia de las garantías secundarias institucionales. Al amparo del Código Civil Federal (Cámara de Diputados del H. Congreso de la Unión, 1928), se explorará el tránsito impostergable de una responsabilidad subjetiva caduca probada (Art. 1910) hacia una responsabilidad civil objetiva, fundada en el riesgo latente que detona la opacidad algorítmica (Art. 1913). Finalmente, se expondrá la imperiosa

necesidad de incorporar el criterio de *targeting* —entendido como la aplicación extraterritorial de la ley a corporaciones que dirigen u orientan deliberadamente sus servicios hacia consumidores nacionales— para someter materialmente a las entidades foráneas a la soberanía jurisdiccional mexicana.

La complejidad multidimensional del fenómeno exige una aproximación metodológica de doble espectro. Consecuentemente, el estudio se estructura bajo un diseño mixto explicativo secuencial (CUAL-cuan), cimentado en la premisa irrenunciable de que toda deconstrucción dogmática debe anclarse en evidencia empírica tangible e irrefutable.

FASE CUALITATIVA

Se desplegó un diseño de investigación jurídico-documental con un corte crítico-hermenéutico. La unidad de análisis abarcó el núcleo normativo primario: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el Código Civil Federal (CCF) de México, contrastándolos analíticamente con las disposiciones del Reglamento General de Protección de Datos (RGPD) emitido por el Parlamento Europeo y el Consejo de la Unión Europea (2016). A nivel jurisprudencial, la disección recayó sobre los agudos razonamientos esgrimidos en la Acción de Inconstitucionalidad 82/2021 del Pleno de la Suprema Corte de Justicia de la Nación (2022), relativa al fallido Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), y se utilizó como parámetro estricto de control de constitucionalidad *a fortiori*.

FASE CUANTITATIVA

Para evidenciar empíricamente la nulidad material del consentimiento expreso ante los tribunales, se diseñó un análisis de contenido transversal y no reactivo. La población objetivo radicó en las "políticas de privacidad" y los "términos de servicio" de las corporaciones tecnológicas de mayor penetración y dominio en el territorio mexicano. Se extrajo una muestra por conveniencia de quince casos paradigmáticos ($N=15$), que abarcaban titanes de los sectores de redes sociales, comercio electrónico y plataformas de entretenimiento a la carta.

La codificación estructuró tres variables independientes, cuyo propósito singular fue medir objetivamente la carga cognitiva exigida al usuario medio:

- Extensión (V1): Cuantificación absoluta del número de palabras.

- Legibilidad (V2): Aplicación de la fórmula de legibilidad de Flesch-Szigriszt, validada métricamente para el idioma español (Szigriszt Pazos, 2001), que arroja un índice numérico en el que valores inferiores indican una barrera de dificultad sintáctica y semántica más alta.
- Complejidad referencial (V3): Conteo estricto de hipervínculos activos que redirigen a normativas accesorias o complementarias, diseminando maliciosamente la integralidad del contrato maestro.

DESARROLLO Y DISCUSIÓN

ARQUITECTURA DEL CONSENTIMIENTO: RIGOR FORMAL FRENTE A LA ASIMETRÍA MATERIAL

El análisis normativo de los artículos 7 y 8 de la LFPDPPP revela que el sistema jurídico mexicano se articula en torno a la exigencia de consentimiento expreso para el tratamiento de datos personales, el cual se verifica mediante la aceptación explícita del usuario al marcar la casilla de verificación en las plataformas. Sin embargo, esta estructura, aparentemente garantista, colapsa ante la realidad operativa del ecosistema digital. Los resultados del análisis cuantitativo de los quince casos paradigmáticos indican que el usuario promedio redacta 5,070 palabras por documento. Sumado a una complejidad lingüística situada en el rango de "algo difícil" (promedio de Flesch de 53.18) —que exige niveles de instrucción universitaria para su adecuada comprensión—, el consentimiento se convierte en un acto volitivo desprovisto de información real.

Esta saturación cognitiva no constituye un error técnico, sino una estrategia deliberada que configura cláusulas contractuales abusivas. El problema jurídico central no es la inexistencia de un consentimiento expreso, sino la inoperancia de este bajo esquemas de adhesión que impiden la autodeterminación informativa. Por tanto, la calificación de "contratos fraudulentos" debe transitar hacia la noción técnica de "cláusulas contractuales abusivas", entendidas como aquellas que, en contra de la buena fe, causan un desequilibrio sustancial en los derechos y obligaciones de las partes en perjuicio del consumidor.



ASIMETRÍA ALGORÍTMICA Y LA BARRERA DE LA CULPA EN LA RESPONSABILIDAD CIVIL

La determinación del daño moral derivado de la vulneración de datos enfrenta obstáculos probatorios insuperables bajo el régimen de responsabilidad subjetiva previsto en el Artículo 1910 del Código Civil Federal. El usuario se encuentra en la imposibilidad de acreditar la culpa o la negligencia específica del prestador de servicios en el diseño de un algoritmo opaco. Para superar esta barrera, la dogmática jurídica debe avanzar hacia la aplicación del Artículo 1913 del mismo ordenamiento, que regula la responsabilidad por el uso de mecanismos o instrumentos peligrosos.

La perfilación algorítmica y la manipulación del comportamiento deben ser interpretadas por la judicatura como actividades de riesgo creado, dada la naturaleza intrínsecamente opaca y el potencial lesivo de los sistemas de inteligencia artificial utilizados por las plataformas. Al tratarse de una actividad riesgosa por definición, quien lucra con el manejo masivo de datos debe responder por los daños que genere, independientemente de la prueba de su culpa, invirtiendo así la carga de la prueba en favor del titular vulnerado.

EFICACIA SANCIONADORA Y DISUASIÓN ECONÓMICA: UN ANÁLISIS COMPARATIVO

El vértice administrativo de la LFPDPPP, gestionado por el INAI, enfrenta severas limitaciones en su eficacia. Mientras que el INAI ha impuesto multas que, si bien son históricas a nivel nacional (por ejemplo, 60.6 millones de pesos en el caso Cambridge Analytica), resultan financieramente irrelevantes para corporaciones de alcance global, el modelo sancionatorio estadounidense refleja una capacidad disuasoria cualitativamente superior. A modo de contraste, la Federal Trade Commission (FTC) impuso a Facebook una sanción de 5 mil millones de dólares por prácticas similares. Esta disparidad evidencia que el esquema mexicano opera actualmente como un "costo operativo" aceptable para las plataformas, y no como una garantía secundaria eficaz que disuada la reincidencia en el uso indebido de la información.

JURISDICCIÓN DIFUSA Y EL CRITERIO DE EXTRATERRITORIALIDAD (TARGETING)

La eficacia del marco jurídico se ve mermada por la ambigüedad de su alcance territorial frente a plataformas que operan a nivel global. Para mitigar



este vacío legal, resulta imperativa la adopción del criterio de targeting o direccionamiento de servicios, técnica que otorga alcance extraterritorial a la norma cuando una entidad, independientemente de su lugar de establecimiento, orienta deliberadamente sus servicios hacia los consumidores nacionales. Esta figura permitiría que la autoridad mexicana sometiera a escrutinio efectivo a las plataformas que, aunque carecen de domicilio fiscal en el país, lucran con el tratamiento de datos de usuarios residentes en México, homologando nuestra práctica a los estándares del RGPD europeo.

ANATOMÍA COMPARADA DEL CONSENTIMIENTO: EL ABISMO ENTRE LA LFPDPPP Y EL RGPD

El contraste normativo desnuda la inoperancia dogmática del marco legislativo mexicano. Mientras la LFPDPPP petrifica la manifestación de la voluntad en una dicotomía binaria que acorrala al usuario entre la aceptación total y la exclusión del servicio (Cámara de Diputados del H. Congreso de la Unión, 2010), el paradigma transatlántico evolucionó hacia la protección material. El Reglamento General de Protección de Datos instauró un rigor analítico ineludible, exigiendo que el consentimiento sea libre, específico, informado e inequívoco mediante una clara acción afirmativa (Parlamento Europeo y Consejo de la Unión Europea, 2016). La normativa europea prohíbe taxativamente las casillas premarcadas y el condicionamiento del contrato a la entrega de datos innecesarios. En México, esta granularidad no existe. La Suprema Corte de Justicia de la Nación (2022) ya delineó un precedente severo sobre la recolección desproporcionada de información en la Acción de Inconstitucionalidad 82/2021; si el máximo tribunal determinó que el Estado no puede coaccionar la entrega de datos biométricos bajo la premisa de seguridad nacional, resulta un contrasentido jurídico que entidades privadas transnacionales lo hagan impunemente bajo el escudo del lucro mercantil. El consentimiento en México, atrapado en una redacción legalista de 2010, claudica ante la arquitectura predatoria de las interfaces contemporáneas.

TAXONOMÍA DE LA OPACIDAD: DESPLIEGUE EMPÍRICO DE LAS PLATAFORMAS

La disección de la matriz cuantitativa (tabla 1) revela patrones corporativos altamente diferenciados que evidencian un diseño deliberado del laberinto cognitivo. Por un lado, los titanes del software y el comercio electrónico



apuestan por la asfixia volumétrica. Microsoft encabeza el espectro con un documento titánico de 15,502 palabras, seguido de cerca por Coppel con 11,180. Pretender que un consumidor asimile un contrato equiparable en extensión a una tesina universitaria antes de instalar un sistema operativo carece de toda lógica fáctica. Por otro lado, entidades basadas en la segmentación algorítmica para la venta de publicidad, como Google y Meta, emplean la táctica de fragmentación referencial. Al incrustar 88 y 39 hipervínculos activos respectivamente, dinamitan la unidad del documento maestro. El usuario es arrojado a un abismo de políticas accesorias, anexos de privacidad y adendas territoriales, lo que diluye la posibilidad humana de rastrear el destino final de sus metadatos. Finalmente, el sector de la economía colaborativa y el *streaming* (DiDi, Uber, Netflix) presenta textos considerablemente más breves, pero la trampa subyace en su métrica Flesch-Szigriszt (Szigriszt Pazos, 2001). Ninguno de los quince casos analizados logra descender a un rango de "Lectura Normal". Todos orbitan entre lo "Algo Difícil" y lo "Difícil", erigiendo una barrera técnica y semántica que convierte el acto de aceptar en un salto al vacío.

ALGORITMOS COMO MECANISMOS PELIGROSOS: LA DOGMÁTICA DEL ARTÍCULO 1913 DEL CCF

Trasladar la responsabilidad civil objetiva al ecosistema digital exige audacia judicial y una reinterpretación teleológica de la norma. Históricamente, el Artículo 1913 del Código Civil Federal (Cámara de Diputados del H. Congreso de la Unión, 1928) fue concebido para resarcir daños ocasionados por artefactos tangibles cuya velocidad, naturaleza explosiva o energía eléctrica representaran un riesgo inherente para la sociedad. Hoy, el concepto de "mecanismo peligroso" debe desprenderse de su envoltura física. Un algoritmo opaco, diseñado para la extracción masiva, el cruce psicográfico de vulnerabilidades y la perfilación predictiva, constituye una herramienta de alto riesgo estructural. La asimetría es insalvable. El titular de los datos jamás tendrá acceso al código fuente de la plataforma ni comprenderá la ruta automatizada que siguió su información para causar un daño moral o patrimonial. Exigirle que pruebe la "culpa" o la negligencia procedimental de la corporación bajo el régimen subjetivo tradicional es condenarlo a una *probatio diabolica*. Al catalogar la perfilación transnacional como una actividad riesgosa por definición, el ordenamiento jurídico mexicano facultaría a los tribunales para revertir la carga probatoria, obligando a la



empresa a indemnizar el daño producido por el solo hecho de lucrar con un sistema de inteligencia artificial cuyo control escapa al entendimiento público.

Tabla 1. Matriz de Resultados Cuantitativos (N= 15)

#	Empresa (Caso-Tipo)	V1: Extensión (Palabras)	V2: Legibilidad (Flesch)	Rango (Dificultad)	V3: Complejidad (Links)
1	Microsoft	15,502	59.25	algo difícil	61
2	Coppel	11,180	57.73	algo difícil	23
3	Spotify	6,512	54.03	algo difícil	27
4	Rappi	6,131	56.36	algo difícil	3
5	TikTok	5,404	51.22	algo difícil	15
6	Amazon	4,851	49.54	difícil	18
7	Meta (Facebook)	4,197	50.94	algo difícil	39
8	YouTube	4,183	58.41	algo difícil	32
9	Google	3,410	50.37	algo difícil	88
10	Uber	3,353	55.01	algo difícil	5
11	Nefflix	3,015	54.98	algo difícil	9
12	X (Twitter)	2,730	57.39	algo difícil	20
13	Apple	2,028	53.07	algo difícil	6
14	Disney+	2,036	44.56	difícil	21
15	DiDi	1,529	44.90	difícil	2
	Promedios:	5,070.73	53.18	algo difícil	24.60

CONCLUSIONES

La presente investigación ha demostrado, mediante un diseño metodológico mixto, que el modelo de "consentimiento informado" que rige la economía digital en México constituye una ficción jurídica, teórica y material. La rigidez del sistema, al aferrarse a una interpretación formalista del consentimiento expreso, desatiende la realidad fáctica de la asimetría de poder entre el consumidor y los titanes tecnológicos.

Se concluye que la ineficacia del marco jurídico no radica en la ausencia de normas, sino en su diseño estructural. Los hallazgos confirman tres falencias determinantes:



Ineficacia del consentimiento: el acto de aceptación es materialmente imposible de otorgar de forma informada cuando el consumidor enfrenta barreras de extensión, legibilidad técnica y fragmentación referencial que exceden las capacidades cognitivas del ciudadano promedio.

Insuficiencia sancionadora: el esquema de multas actual carece de fuerza disuasoria frente a corporaciones transnacionales y opera como un costo operativo mínimo en comparación con los beneficios derivados de la explotación de datos.

Barreras probatorias: el sistema de responsabilidad subjetiva impone al titular una carga probatoria de "culpa", lo que deriva en una *probatio diabolica*, dada la opacidad intrínseca de los algoritmos utilizados para la perfilación.

La protección efectiva de la autodeterminación informativa requiere una transformación paradigmática. En primer lugar, es indispensable transitar hacia un modelo de responsabilidad civil objetiva, fundada en el riesgo creado, desplazando la carga de la prueba a quienes lucran con la opacidad algorítmica. En segundo lugar, se requiere la adopción explícita del criterio de targeting en la LFPDPPP, lo cual permitirá otorgar alcance extraterritorial a la ley y someter a las plataformas transnacionales a la soberanía jurisdiccional mexicana.

Finalmente, esta investigación insta a abandonar el paradigma del consentimiento individual como única vía de protección. Se propone la implementación de una responsabilidad fiduciaria digital, en la que las plataformas, al gestionar activos personales, asuman obligaciones de cuidado que prohíban usos perjudiciales, independientemente de lo pactado en contratos de adhesión ilegibles. Solo mediante estas reformas estructurales se podrá cerrar la brecha de eficacia que actualmente permite la explotación desmedida de la información en el ecosistema digital.

REFERENCIAS

- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058.
<https://doi.org/10.1016/j.tele.2017.04.013>

- Cámara de Diputados del H. Congreso de la Unión. (1928). *Código Civil Federal*.
https://www.diputados.gob.mx/LeyesBiblio/pdf/2_110121.pdf
- Cámara de Diputados del H. Congreso de la Unión. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.
<https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 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*.
<http://data.europa.eu/eli/reg/2016/679/oj>
- Suprema Corte de Justicia de la Nación. (2022). *Sentencia dictada por el Tribunal Pleno de la Suprema Corte de Justicia de la Nación en la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021*. Diario Oficial de la Federación.
<https://sidof.segob.gob.mx/notas/5673910>
- Szigriszt Pazos, F. (2001). *Sistemas predictivos de legibilidad del mensaje escrito: Fórmula de perspicuidad* [Tesis doctoral, Universidad Complutense de Madrid]. Docta Complutense. <https://docta.ucm.es/entities/publication/72b6bb4b-0773-4ca2-84f6-748c83076a> ce