ICU Investigación, Ciencia y Universidad ISSN 2525-1783

http://revistas.umaza.edu.ar/index.php/icu/index | Número Temático IV: Desarrollo Sostenible | Año 2026 / Vol 10 - Nº 15

Primer puesto Área Derechos y Sociedad

Modelos europeo y chino frente a la manipulación política digital: tensiones entre autonomía y soberanía

European and Chinese Models Facing Digital Political Manipulation: Tensions between Autonomy and Sovereignty

Martínez Funes, Andrea Carolina

Universidad Blas Pascal. Instituto de Investigación en Ciencias Jurídicas; Argentina.

Correo de correspondencia: amartinezfunes@gmail.com

Recepción: 14/11/2025
Aceptación: 12/01/2026
Publicación: 06/03/2026

Palabras clave: Protección de datos personales; Manipulación política digital; Derecho comparado; Inteligencia artificial
Keywords: *Personal data protection; Digital political manipulation; Comparative law; Artificial intelligence*

DOI: https://doi.org/10.59872/icuv10i15.594

Resumen

El tratamiento automatizado de datos personales para microsegmentación política digital plantea desafíos regulatorios sin precedentes para la protección de derechos fundamentales. Este trabajo examina comparativamente cómo el Reglamento General de Protección de Datos europeo y la Ley de Protección de Información Personal china establecen límites a estas prácticas desde concepciones opuestas sobre autonomía informativa y soberanía estatal. Se utilizó metodología cualitativa de análisis jurídico-comparado funcional, examinando disposiciones normativas principales, principios rectores, mecanismos de garantía y excepciones de ambos marcos. Los resultados revelan convergencias formales significativas en categorías como consentimiento, transparencia y limitación de finalidad, pero divergencias funcionales profundas en su estructura de garantías e independencia institucional. El marco europeo estructura protecciones donde la autonomía individual opera como derecho fundamental que limita el poder estatal, mientras el marco chino estructura protecciones donde la seguridad estatal opera como valor jerárquicamente superior. El marco europeo enfrenta limitaciones técnicas derivadas de la opacidad algorítmica persistente, mientras el marco chino enfrenta limitaciones institucionales por ausencia de independencia de órganos de control. Se concluye que la convergencia regulatoria global oculta divergencias estructurales profundas enraizadas en concepciones políticas y filosóficas opuestas sobre protección de datos en contextos de manipulación política digital.

Abstract

Automated processing of personal data for digital political microtargeting poses unprecedented regulatory challenges for protecting fundamental rights. This work comparatively examines how the European General Data Protection Regulation and the Chinese Personal Information Protection Law establish limits to these practices from opposed conceptions of information autonomy and state sovereignty. Qualitative methodology of functional comparative legal analysis was employed, examining primary normative provisions, guiding principles, protection mechanisms, and exceptions of both frameworks. Results reveal significant formal convergences in categories such as consent, transparency, and purpose limitation, but profound functional divergences in their protection structures and institutional independence. The European framework structures protections where individual autonomy operates as a fundamental right limiting state power, while the Chinese framework structures protections where state security operates as a hierarchically superior value. The European framework faces technical limitations derived from persistent algorithmic opacity, while the Chinese framework faces institutional limitations due to absence of supervisory body independence. It is concluded that global regulatory convergence obscures profound structural divergences rooted in opposed political and philosophical conceptions about data protection in contexts of digital political manipulation.

Cómo citar: Martinez Funes, A. (2026). Modelos europeo y chino frente a la manipulación política digital: tensiones entre autonomía y soberanía: European and Chinese Models Facing Digital Political Manipulation: Tensions between Autonomy and Sovereignty. Investigación Ciencia Y Universidad, 10(15), 22–28. https://doi.org/10.59872/icu.v10i15.594

Introducción

El tratamiento automatizado de datos personales para fines de microsegmentación política digital plantea desafíos regulatorios sin precedentes en democracias contemporáneas. Esta transformación no es meramente tecnológica, sino que entraña profundas implicaciones para la protección de derechos fundamentales. Solove (2006) desarrolló una taxonomía comprehensiva de los daños derivados del recopilamiento y uso de información personal; O'Neil (2016) documentó cómo algoritmos sin control adecuado operan particularmente como «armas de destrucción matemática» en contextos de influencia política. A los efectos de este trabajo, entendemos «manipulación política digital» como el tratamiento automatizado de datos personales para crear perfiles comportamentales orientados a *microtargeting* electoral. Por «límites que establecen» nos referimos a las restricciones normativas concretas que cada marco establece respecto a qué prácticas están prohibidas, qué garantías deben proporcionarse a sujetos de datos, qué excepciones se admiten, y quién ostenta poder de decisión en caso de conflicto. Esta delimitación operativa permite examinar cómo dos marcos normativos responden a un problema común -proteger derechos en contextos de tratamiento automatizado politizado- desde fundamentos regulatorios divergentes.

La divergencia entre el modelo europeo y el modelo chino enraíza en concepciones fundamentalmente distintas sobre autonomía informativa y soberanía estatal. Warren y Brandeis (1890) iniciaron la tradición de protección de la privacidad como derecho individual autónomo. Nissenbaum (2009) avanzó hacia el concepto de «integridad contextual», reconociendo que la protección debe respetar normas y expectativas específicas de privacidad en distintos contextos. Schneider (2018) analiza cómo el tecnonacionalismo, particularmente en China, concibe datos personales como activos estratégicos de seguridad nacional subordinados al interés estatal. Zuboff (2019) caracteriza estas dinámicas como parte de un «capitalismo de vigilancia» donde la acumulación masiva de dato genera poder político con riesgos simultáneamente individuales y colectivos. La tensión entre autonomía informativa -derecho del sujeto a controlar información sobre sí mismo- y soberanía estatal -autoridad del Estado sobre flujos informativos e infraestructuras digitales- no es meramente teórica, sino que genera estructuralmente las divergencias regulatorias observables en distintas jurisdicciones.

La respuesta normativa a estos desafíos ha adoptado geografías regulatorias contrastantes. El GDPR, promulgado en 2016 y vigente desde 2018, estructura prioritariamente protecciones centradas en la autonomía individual mediante mecanismos de garantía de control, transparencia y responsabilidad del responsable del tratamiento. De Vidales (2025) examina específicamente cómo disposiciones del GDPR relativas a decisiones individuales automatizadas constituyen restricciones normativas orientadas a limitar *microtargeting* electoral, aunque identifica limitaciones técnicas significativas. Por su parte, China promulgó en 2021 la Ley de Protección de Información Personal (PIPL) y la Ley de Seguridad de Datos (DSL), seguidas por las Disposiciones sobre Recomendaciones Algorítmicas (2022). Aunque formalmente estas normas incorporan categorías análogas a las europeas -consentimiento, transparencia, limitación de finalidad, responsabilidad- su estructura subyacente subordina sistemáticamente estos mecanismos a consideraciones de seguridad nacional y control estatal. Creemers (2020) documenta cómo en el marco chino, la protección de datos está estructurada subordinada a objetivos de orden público y seguridad estatal. Ambos marcos regulan categorías similares pero con prioridades normativas radicalmente distintas.

El análisis de ambos marcos frente al *microtargeting* político permite identificar convergencias formales -la adopción de categorías jurídicas comunes- pero también divergencias funcionales significativas en cómo estructuran garantías, excepciones y distribución del poder de decisión. Metcalf, Moss y Boyd (2021) demuestran que esta brecha entre formalismo normativo e implementación efectiva es particularmente aguda en materia de institucionalización de estándares éticos. La pregunta de investigación que estructura este trabajo es: ¿Difieren el GDPR y la PIPL en los límites que establecen al tratamiento automatizado de datos personales en contextos de manipulación política digital, a la luz de la autonomía informativa y la soberanía estatal? El objetivo es examinar comparativamente cómo ambos marcos regulan el tratamiento automatizado de datos personales orientado a microsegmentación política, identificando convergencias en sus estructuras formales y divergencias en sus mecanismos de garantía, excepciones y distribución del poder de supervisión. Se prestará especial atención a cómo cada marco articula la relación entre autonomía informativa individual y soberanía estatal, entendiendo que esta articulación explica las divergencias funcionales observables. La hipótesis que guía este análisis sostiene que el GDPR y la PIPL convergen en la adopción de categorías formales comunes, pero divergen sustancialmente en su estructura funcional de garantías y excepciones, derivando estas divergencias de concepciones opuestas sobre autonomía informativa y soberanía estatal. Mientras que el GDPR estructura prioritariamente protecciones centradas en la autonomía individual mediante garantías de control y transparencia, la PIPL subordina estas protecciones a consideraciones de seguridad nacional y control estatal. Consecuentemente, ambos marcos enfrentan limitaciones funcionales distintas para contener manipulación política digital: en el GDPR, limitaciones técnicas derivadas de la opacidad algorítmica y dificultades prácticas de consentimiento genuinamente informado; en la PIPL, limitaciones institucionales derivadas de ausencia de independencia de órganos de control y preeminencia estructural de seguridad estatal sobre derechos individuales.

Materiales y Métodos

Esta investigación adopta una metodología cualitativa de carácter jurídico-comparado orientada al análisis hermenéutico de fuentes normativas y doctrinarias. El enfoque comparatista funcional examina cómo sistemas jurídicos distintos resuelven problemas similares mediante equivalentes funcionales, permitiendo caracterizar cómo el GDPR europeo y la PIPL china establecen límites al tratamiento automatizado de datos personales en contextos de manipulación política digital.

Las fuentes primarias analizadas comprenden el Reglamento (UE) 2016/679 (GDPR) y la Ley de Protección de Información Personal (PIPL) de 2021, como instrumentos regulatorios principales mediante los cuales ambas jurisdicciones establecen límites al tratamiento automatizado de datos personales en contextos de manipulación política digital. El análisis examina cómo cada marco articula la relación entre autonomía informativa (derechos individuales) y soberanía estatal (seguridad nacional) en la regulación del tratamiento automatizado, identificando principios, mecanismos de garantía y excepciones normativas. Se utilizan como fuentes secundarias contextuales documentos interpretativos emitidos por autoridades supervisoras europeas (Autoridad Europea de Protección de Datos, Comisión Europea) y chinas (*Cyberspace Administration of China*) para aclarar disposiciones principales, sin constituir objeto de análisis comparativo independiente.

Las fuentes doctrinarias comprenden literatura clásica sobre autonomía informativa y control de datos, literatura especializada en soberanía digital y tecnonacionalismo en contextos asiáticos, y literatura contemporánea sobre inteligencia artificial aplicada a contextos electorales. Esta base bibliográfica permite fundamentar categorías conceptuales y contextualizar los desafíos que plantea la manipulación política digital para ambos marcos regulatorios.

El procedimiento de análisis se estructuró en tres fases. En la primera, se realizó análisis gramatical y sistemático de disposiciones normativas de ambos marcos, identificando principios rectores explícitamente enunciados, mecanismos de garantía establecidos para sujetos de datos (consentimiento, derechos de acceso y rectificación, evaluaciones de impacto), y excepciones expresamente previstas respecto a seguridad pública y seguridad nacional. En la segunda fase, se procedió al análisis funcional, que examina la estructura normativa de cómo cada marco se orienta a limitar tratamiento automatizado en contextos de manipulación política, evaluando consistencia interna y resolución de tensiones entre protecciones individuales y objetivos estatales. Este análisis funcional se limita a evaluar la estructura normativa y no su nivel de cumplimiento fáctico o eficacia práctica, siendo por tanto un análisis de disposiciones en términos normativos. En la tercera fase, se realizó análisis comparativo mediante interpretación sistemática y teleológica, identificando convergencias formales (categorías jurídicas comunes) y divergencias funcionales (diferencias en estructura de garantías, independencia institucional de órganos supervisores, jerarquía normativa cuando existe conflicto entre autonomía individual y seguridad estatal).

El análisis no incorpora métodos estadísticos dado que el objeto de estudio es fundamentalmente textual -la estructura normativa de dos marcos regulatorios- y no empírico-cuantitativo. Sin embargo, el análisis hermenéutico-funcional adopta estándares de rigurosidad mediante análisis textual preciso, distinción sistemática entre lo prescriptivo y lo inferido, y criterios explícitos para clasificación de convergencias y divergencias. El enfoque reconoce que interpretación de normas jurídicas es situada, pero minimiza sesgo mediante perspectivas doctrinarias diversas, examen de documentos de autoridades supervisoras en ambas jurisdicciones, e identificación explícita de limitaciones: restricción a marcos formales sin examinar implementación práctica, mediación interpretativa en traducción de documentos chinos, y carácter preliminar de conclusiones respecto a regulación emergente de inteligencia artificial.

Resultados

El análisis comparativo de los límites normativos que el GDPR y la PIPL establecen al tratamiento automatizado de datos personales en contextos de manipulación política digital revela una estructura regulatoria compleja en ambas jurisdicciones, caracterizada por convergencias formales significativas pero divergencias funcionales profundas en sus mecanismos de garantía y excepciones.

El GDPR estructura el tratamiento de datos personales sobre principios explícitos enunciados en su Artículo 5, estableciendo como pilares fundamentales la licitud, la transparencia y la responsabilidad del responsable del tratamiento. Respecto al tratamiento automatizado específicamente, el Artículo 22 GDPR prohíbe las decisiones individuales automatizadas que produzcan efectos jurídicos o similares sobre interesados, salvo en casos excepcionales explícitamente limitados: ejecución de contrato, autorización legal, o consentimiento explícito del interesado. Las excepciones normativas en materia de seguridad nacional y orden público quedan limitadas por disposiciones que exigen proporcionalidad, necesidad, y control judicial previo o posterior. El artículo 35 GDPR requiere evaluaciones de impacto en la protección de datos (DPIA) cuando se procesan datos de categorías especiales o mediante tratamiento automatizado en larga escala. Las autoridades de control -autoridades independientes con autonomía operativa y financiera- están investidas de poder de decisión vinculante y tienen capacidad de imposición de sanciones administrativas.

La PIPL establece en su Artículo 5 que los principios del procesamiento de información personal son legalidad, propósito legítimo, minimización de datos, exactitud y seguridad. Sin embargo, estos principios se articulan dentro de un marco donde la seguridad nacional y la estabilidad social constituyen excepciones prevalentes. El Artículo 26 PIPL regula decisiones automatizadas, permitiendo el procesamiento automatizado para perfilar a interesados pero requiriendo consentimiento y medidas de protección. A diferencia del GDPR, la PIPL en su Artículo 34 expresamente autoriza excepcionalmente el procesamiento sin consentimiento cuando la información personal se obtiene para «cumplir con obligaciones legales, fines de seguridad nacional, defensa nacional, seguridad pública, orden público, asuntos de interés público importante». Estas excepciones, a diferencia del GDPR, no requieren evaluación individual de proporcionalidad, sino que son categóricamente autorizadas cuando se declara alguno de estos fines. Las autoridades de control en la PIPL operan bajo estructura jerárquica estatal -*la Cyberspace Administration of China* (CAC) y otras autoridades están integradas dentro de la administración estatal y reportan a órganos superiores- sin independencia institucional comparable a la del GDPR.

Ambos marcos convergen formalmente en la adopción de categorías jurídicas comunes. El consentimiento aparece en ambos como mecanismo central de licitud del tratamiento. Transparencia y derechos de acceso constituyen componentes del marco regulatorio en ambas jurisdicciones. La limitación de finalidad -el principio de que datos recolectados para un propósito no pueden ser utilizados para otros sin nueva justificación- está presente en ambos marcos. Evaluaciones de impacto previas o consentimientos informados constituyen requisitos nominales en ambas legislaciones. Esta convergencia formal sugiere una respuesta común a desafíos técnicos y políticos similares del tratamiento automatizado de datos personales.

Sin embargo, las divergencias funcionales son significativas. En el GDPR, el consentimiento debe ser libre, específico, informado e inequívoco, exigiendo al responsable del tratamiento demostrabilidad del consentimiento obtenido de forma activa. En la PIPL, el consentimiento es requisito formal que no precluye excepciones por seguridad nacional o estabilidad social: un individuo puede consentir al procesamiento de sus datos, pero el Estado puede aún utilizar esos datos por consideraciones de seguridad nacional sin necesidad de consentimiento individual adicional. En el GDPR, las excepciones por seguridad pública y orden público constituyen limites estrictamente interpretados bajo principios de proporcionalidad y necesidad. En la PIPL, las excepciones por seguridad nacional, defensa nacional y orden público operan como categorías amplias de autorización categórica que no requieren justificación individual de proporcionalidad.

La independencia institucional de órganos supervisores constituye una divergencia funcional significativa en la estructura de ambos marcos. Se hipotetiza que esta independencia facilita (aunque no garantiza necesariamente) la contención de manipulación política digital, porque permite que autoridades actúen sin presiones políticas de gobiernos. Sin embargo, esta relación causal es un mecanismo potencial no demostrado empíricamente en este trabajo: es posible tener autoridades independientes con marcos débiles (poca contención) o autoridades dependientes con marcos fuertes (potencialmente mayor contención). Este análisis identifica la diferencia estructural pero no resuelve la cuestión de su efectividad real. El GDPR requiere que autoridades de protección de datos sean independientes, libres de influencia externa, con autonomía operativa y financiera, y con poder de decisión vinculante en materias de protección de datos. Estas autoridades operan dentro de la Unión Europea bajo marcos donde el Tribunal de Justicia de la Unión Europea puede revisar sus decisiones, pero fundamentalmente son autónomas. En la PIPL, la CAC y otras autoridades supervisoras de protección de datos son órganos integrados dentro de la administración estatal y reporta a estructuras jerárquicas superiores, sin independencia formal comparable. Esto significa que decisiones sobre protección de datos pueden estar subordinadas a consideraciones de política pública estatal más amplias.

La resolución de conflictos entre protección individual de datos y objetivos estatales se estructura de manera opuesta en ambos marcos. En el GDPR, cuando existe conflicto entre un derecho individual a protección de datos y una medida de seguridad pública, el marco presupone que los derechos individuales deben ser protegidos como posición de preferencia, siendo las excepciones casos debidamente justificados y limitados. En la PIPL, el conflicto se resuelve por subordinación de protecciones individuales a consideraciones de seguridad nacional y orden público, conceptualizadas como prioridades públicas mayores que derechos individuales. Esta diferencia estructural refleja una distinta ponderación de qué valor regulatorio es preponderante: autonomía individual del sujeto de datos (GDPR) versus soberanía estatal sobre infraestructuras de datos (PIPL).

El análisis normativo también revela que ambos marcos enfrentan limitaciones específicas en su capacidad de contener manipulación política digital. El GDPR establece límites mediante prohibición de decisiones individuales automatizadas, requerimiento de transparencia algorítmica, y exigencia de evaluaciones de impacto. Sin embargo, estas limitaciones operan a nivel de estructura normativa -lo que las normas dicen que debe ocurrir- sin necesariamente garantizar que los algoritmos de manipulación política sean técnicamente indetectables que la transparencia requerida sea operacionalmente posible de materializar en sistemas complejos. La PIPL establece limitaciones diferentes: autorización categórica de procesamiento por razones de seguridad nacional, sin requerir demostración caso por caso de necesidad, significa que manipulación política digital puede ser legalmente autorizada bajo justificación de seguridad estatal. Ambas limitaciones son limitaciones normativas, estructurales, no empíricas de efectividad real.

Discusión

Los resultados del análisis comparativo revelan que, mientras el GDPR y la PIPL adoptan convergencias formales significativas en sus categorías regulatorias, sus estructuras funcionales divergen de manera profunda en formas que reflejan concepciones opuestas sobre autonomía informativa y soberanía estatal. Esta divergencia funcional, aunque no siempre evidente en la lectura superficial de disposiciones comunes, emerge cuando se examina cómo ambos marcos resuelven conflictos entre protección individual y objetivos estatales. La hipótesis inicial, que sostenía que ambos marcos divergen en su estructura funcional de garantías y excepciones derivado de concepciones opuestas sobre autonomía/soberanía, encuentra confirmación parcial en estos hallazgos, aunque con matices que requieren especificación.

La convergencia formal en categorías como consentimiento, transparencia y limitación de finalidad sugiere, a primera vista, una homogeneización regulatoria global respecto a protección de datos. Metcalf, Moss y Boyd (2021) caracterizaron esta aparente convergencia como resultado de presión normativa internacional y difusión de marcos regulatorios que generan isomorfismo institucional. Sin embargo, el análisis funcional revela que esta convergencia formal oculta divergencias estructurales. El consentimiento en el GDPR opera como mecanismo de autonomía individual: requiere que el sujeto ejerza poder de decisión genuino, acceso a información clara, y capacidad de retracción. En la PIPL, el consentimiento es re-

quisito formal que no precluye excepciones categóricas por seguridad nacional o estabilidad social. Creemers (2020) documenta extensamente cómo en el marco chino, la protección de datos se concibe como instrumento subordinado a objetivos de seguridad estatal. Esta diferencia no es meramente técnica, sino que refleja una jerarquía axiológica distinta: en el GDPR, la autonomía individual opera como derecho fundamental que limita el poder estatal; en la PIPL, la seguridad estatal opera como principio preponderante que condiciona la protección individual.

Es importante reconocer que la caracterización de esta divergencia como «autonomía vs. soberanía» no es la única lectura posible del fenómeno. Un análisis desde perspectivas jurídicas alternativas podría sostener que ambos marcos son igualmente protectores, solo que bajo principios distintos y legítimos: el GDPR prioriza autonomía individual como valor jurídico fundamental (coherente con tradiciones liberales europeas); la PIPL prioriza seguridad estatal como valor colectivo preponderante (coherente con tradiciones de gobernanza estatal asiáticas). Esto no constituye un juicio de «mejor/peor» sino de jerarquías normativas distintas. Un defensor de la PIPL podría argumentar que la integración de protección de datos en gobernanza estatal representa coherencia institucional, no déficit de protección. Esta diversidad de lecturas interpretativas es característica del derecho comparado riguroso: reconocer que divergencias normativas reflejan opciones legítimas distintas, no deficiencias en un lado u otro.

La estructura de independencia institucional de órganos supervisores constituye un indicador crítico de cómo cada marco resuelve conflictos entre autonomía y soberanía. García González (2010) analiza cómo la independencia de autoridades de protección de datos es elemento estructural que determina si la protección es efectiva o simbólica. El GDPR requiere explícitamente que autoridades de protección de datos sean independientes, libres de influencia externa, con autonomía operativa y financiera. Esta estructura permite que cuando se presenta conflicto entre un derecho individual a protección de datos y una medida de seguridad pública, la autoridad de control pueda actuar como árbitro genuinamente independiente. En la PIPL, la ausencia de independencia institucional de órganos de control significa que conflictos entre protección individual y seguridad estatal se resuelven dentro de estructuras donde la seguridad estatal es valor jerárquicamente superior. Schneider (2018) utiliza el concepto de «tecnonacionalismo» para caracterizar precisamente este fenómeno: la reconfiguración de marcos regulatorios donde infraestructuras de datos son conceptualizadas como activos estratégicos de seguridad nacional subordinados a soberanía estatal. El análisis de PIPL confirma este tecnonacionalismo: no solo regula datos, sino que estructuralmente subordina protecciones individuales a seguridad estatal mediante carencia de independencia institucional.

La hipótesis sobre limitaciones funcionales distintas encuentra confirmación clara. El GDPR enfrenta limitaciones técnicas derivadas de la opacidad algorítmica persistente: aunque requiere transparencia y *explainability*, los sistemas de machine learning complejos permanecen intrínsecamente opacos en aspectos de cómo llegan a decisiones específicas. O'Neil (2016) caracteriza esta opacidad como «armas de destrucción matemática», sistemas que producen daños sin que siquiera el responsable del tratamiento comprenda completamente el mecanismo causal. Estas limitaciones técnicas afectan particularmente al GDPR porque su estructura de protección depende fundamentalmente de consentimiento informado: si el sujeto no puede comprender realmente cómo funcionan los algoritmos, el consentimiento es formalmente dado, pero sustancialmente no genuinamente informado. De Vidales (2025) examina cómo, a nivel de implementación práctica, muchas empresas en la UE satisfacen formalmente requisitos de GDPR sin materializar transparencia efectiva. Estructuralmente, la PIPL difiere del GDPR en que no requiere independencia de órganos supervisores. Esto significa que, según la norma, estas protecciones podrían no ser efectivamente exigibles cuando choquen con decisiones de seguridad nacional. Sin embargo, este análisis no realiza evaluación independiente de implementación práctica; esta conclusión se basa en la estructura normativa, no en análisis empírico de cómo opera en práctica. En este caso, el problema no es técnico sino institucional: las normas existen pero su aplicación puede ser subordinada a consideraciones de seguridad estatal.

El análisis también identifica una limitación metodológica crítica que debe reconocerse: este estudio examina marcos normativos formales sin evaluación de implementación práctica o cumplimiento fáctico. Tanto el GDPR como la PIPL enfrentan brechas significativas entre lo que las normas prescriben y lo que realmente ocurre en la práctica. Metcalf, Moss & Boyd (2021) caracterizan esta brecha como resultado de que instituciones corporativas y estatales frecuentemente desarrollan prácticas que satisfacen formalmente requisitos legales sin materializar protecciones genuinas. Para el GDPR, ello significa que empresas multinacionales pueden cumplir nominalmente requisitos de consentimiento mientras implementan arquitecturas de «dark patterns» que manipulan decisiones. Para la PIPL, significa que la subordinación de protecciones individuales a seguridad estatal puede institucionalizarse de formas que las normas no explícitamente autorizan pero que prácticas burocráticas normalizan. Esta limitación es particularmente importante en contextos de manipulación política digital, donde los efectos prácticos de las regulaciones dependen tanto de implementación como de estructura normativa.
La divergencia funcional identificada tiene implicaciones significativas para la gobernanza de datos personales en contextos de manipulación política digital. Zuboff (2019) advierte sobre el «capitalismo de vigilancia» como fenómeno que combina vigilancia masiva de datos comportamentales con poder político de decisión sobre influencia. En contextos europeos, el GDPR intenta limitar este fenómeno mediante protecciones individuales y exigencia de transparencia. Sin embargo, esas protecciones enfrentan limitaciones técnicas que las hacen incompletas: la opacidad algorítmica significa que incluso sujetos formalmente informados no pueden comprender completamente cómo sus datos se utilizan para su influencia. En contextos chinos, la PIPL opera en marco donde la subordinación estructural de protecciones individuales a seguridad estatal significa que el capitalismo de vigilancia es literalmente institucionalizado: la vigilancia no es solo práctica corporativa

sino principio de gobernanza estatal que las normas autorizan categóricamente. Ambos contextos, manipulación política digital mediante microsegmentación permanece substancialmente sin contención efectiva, aunque por razones distintas: en la UE, por limitaciones técnica que impiden materializar protecciones nominales; en China, porque protecciones individuales están subordinadas a objetivos estatales que pueden autorizar manipulación política como aspecto de gobernanza de seguridad.

Las limitaciones del presente análisis deben reconocerse explícitamente. Primero, el análisis se restringe a marcos formales sin examen de implementación práctica, por lo cual conclusiones sobre «limitaciones funcionales» se refieren a limitaciones en la estructura normativa, no a efectividad real de protecciones. Segundo, el acceso a documentos normativos chinos requirió traducción, introduciendo mediación interpretativa adicional; mientras se emplearon traducciones oficiales y especializadas, la mediación lingüística es fuente de posible sesgo hermenéutico. Tercero, el período analizado (2016-2025) cubre evolución regulatoria continua, particularmente en regulación de inteligencia artificial que está en proceso de transformación, haciendo preliminares conclusiones respecto a normas emergentes (AI Act europeo). Cuarto, este análisis enfatiza marcos estatales sin considerar autorregulación corporativa o estándares privados de gobernanza de plataformas, dimensiones significativas pero que requieren investigación separada. A pesar de estas limitaciones, el análisis proporciona caracterización rigurosa de cómo ambos marcos establecen límites al tratamiento automatizado en contexto de manipulación política digital desde fundamentos conceptuales opuestos.

La aceptación parcial de la hipótesis requiere matización final. La hipótesis planteaba que divergencias derivan de concepciones opuestas sobre autonomía/soberanía, y que ambos marcos enfrentan limitaciones funcionales distintas. El análisis confirma la primera parte: divergencias funcionales derivan efectivamente de autonomía (GDPR) versus soberanía (PIPL) como valores preponderantes. Sin embargo, la segunda parte requiere precisión: no todas las "limitaciones funcionales" son limitaciones del marco normativo, muchas son limitaciones técnicas (opacidad algorítmica) o implementación práctica que transcienden el análisis normativo que este trabajo realiza. Lo que sí puede afirmarse es que el GDPR y la PIPL estructuran protecciones sobre jerarquías de valores distintos. El GDPR estructura protecciones donde autonomía individual opera como derecho fundamental, aunque enfrenta potencialmente tanto limitaciones técnicas (opacidad algorítmica) como limitaciones institucionales (presiones políticas en autoridades). La PIPL estructura protecciones donde seguridad estatal opera como valor jerárquicamente superior, sin requerir independencia institucional de órganos supervisores, lo que añade limitaciones institucionales potenciales a cualquier limitación técnica que también pudiera enfrentar. Ambos marcos probablemente enfrentan el espectro completo de desafíos, no una categoría distinta de limitaciones, pero con diferente peso relativo en su estructura normativa. En ese sentido, la hipótesis encuentra confirmación: divergencias funcionales son reales y derivan de concepciones opuestas sobre autonomía versus soberanía, aunque la efectividad de ambos marcos para contener manipulación política digital enfrenta desafíos que transcienden sus estructuras normativas.

Conclusiones

El análisis comparativo de los límites normativos que el GDPR y la PIPL establecen al tratamiento automatizado de datos personales en contextos de manipulación política digital revela que, a pesar de convergencias formales significativas en categorías como consentimiento, transparencia y limitación de finalidad, ambos marcos divergen funcionalmente en formas profundas. Esta divergencia refleja concepciones opuestas sobre autonomía informativa y soberanía estatal como valores preponderantes: el GDPR estructura protecciones donde la autonomía individual opera como derecho fundamental que limita el poder estatal, mientras la PIPL estructura protecciones donde la seguridad estatal opera como principio jerárquicamente superior que condiciona derechos individuales. Las diferencias en independencia institucional de órganos supervisores, estructura de excepciones, y jerarquía de valores cuando autonomía y seguridad entran en conflicto son indicadores de estas divergencias funcionales fundamentales.

Este análisis aporta al conocimiento jurídico-comparado una caracterización rigurosa de cómo la convergencia regulatoria global en materia de protección de datos oculta divergencias estructurales profundas enraizadas en concepciones políticas y filosóficas opuestas. Demuestra que análisis superficial de isomorfismo institucional -la simple constatación de que marcos adoptan categorías similares- resulta engañoso si no examina críticamente cómo esos marcos funcionan cuando entran en conflicto valores fundamentales. En contextos de manipulación política digital, esto significa que el grado de contención regulatoria no depende solo de categorías nominales sino de cómo los marcos resuelven estructuralmente conflictos entre protección individual y objetivos estatales. Futuras investigaciones deberían examinar implementación práctica de estos marcos y evaluar impacto fáctico de estas divergencias funcionales en protección real de sujetos de datos en contextos electorales.

Referencias Bibliográficas

Alexy, R. (2002). *Teoría de los derechos fundamentales*. Centro de Estudios Políticos y Constitucionales.

Comisión 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* [GDPR]. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2016/679/oj/es

Comisión Europea. (2024). *Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas sobre inteligencia artificial*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/

Creemers, R. (2020). Caught between cybersecurity law and data protection: Personal data and power in China. *Asia Policy, 15*, 38-49.

De Vidales, C. F. M. (2025). Electoral microtargeting: How to protect data from people's political opinions and fight disinformation through EU legislation. *International Journal of Comparative Law, 8*(1), 112-145. https://dialnet.unirioja.es/servlet/articulo?codigo=10370545

Departamento de Ciberseguridad e Informatización de China. (2021a). *Ley de Protección de Información Personal de la República Popular China (PIPL)*. http://www.cac.gov.cn/

Departamento de Ciberseguridad e Informatización de China. (2021b). *Ley de Seguridad de Datos de la República Popular China (DSL)*. http://www.cac.gov.cn/

Departamento de Información de Internet de China. (2022). *Disposiciones sobre la Administración de Recomendaciones Algorítmicas*. http://www.cac.gov.cn/

García González, A. (2010). El derecho a la autodeterminación informativa. *Ius et Praxis, 16*(2), 145-170.

IDEA Internacional. (2024). *La inteligencia artificial y la gestión electoral: Principios para el uso responsable de la IA en elecciones*. https://www.idea.int/

Lyth, K. T., & Thomas, P. (2023). Algorithmic discrimination in electoral contexts: Evidence and mitigation strategies. *Electoral Studies*, 81, 102656. https://doi.org/10.1016/j.electstud.2022.102656

Metcalf, J., Moss, E., & Boyd, D. (2021). Owning ethics: Corporate logics, silicon valley, and the institutionalization of ethics. *Social Research, 88*(2), 449-476.

Michaels, R. (2006). The functional method of comparative law. En M. Reimann & R. Zimmermann (Eds.), *The Oxford handbook of comparative law* (pp. 339-382). Oxford University Press.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishers.

Parlamento Europeo. (2022). *Directiva sobre Servicios Digitales (DSA). Reglamento (UE)* 2022/2065. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/

Schneider, N. (2018). Cybernationalism and digital sovereignty in China. *Journal of Information Technology & Policy, 12*(3), 234-255.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania *Law Review, 154*(3), 477-564. https://doi.org/10.2139/ssrn.313681

UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. https://unesdoc.unesco.org/

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220. https://doi.org/10.2307/1321160

Westin, A. F. (1967). *Privacy and freedom*. Atheneum Publishers.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.