44 JORNADA NOTARIAL BONAERENSE

TEMA 3. EJERCICIO NOTARIAL EN LA ERA DIGITA

Coordinador: Not. Walter C. SCHMIDT (walter.schmidt@notariado.ar)

Subcoordinador: Not. Sebastián LASSALLE (escsebastianlassalle@gmail.com)

El consumidor electrónico hipervulnerable en la era digital: protección jurídica, manipulación algorítmica y contratación electrónica

Autoras: Karina Vanesa Salierno (escribaniasalierno@gmail.com) y Marcela Viviana Spina (escribaniaspina@gmail.com)

Categoría: Trabajos de autores experimentados

Resumen

El presente trabajo analiza la figura del consumidor electrónico hipervulnerable en el contexto de la contratación digital contemporánea, abordando las complejidades jurídicas que emergen de la intersección entre la tecnología algorítmica, la economía de datos y los derechos fundamentales del consumidor. A partir del marco normativo argentino compuesto por la Ley 24.240, Código Civil y Comercial de la Nación (arts. 1092-1095 y 1107-1110), Ley 25.326 y Resolución 139/2020 del SIGEN y del derecho comparado europeo (Reglamento de Inteligencia Artificial (UE) 2024/1689 y Digital Services Act, se examina la situación de colectivos especialmente vulnerables como adultos mayores, personas con discapacidad y niños, niñas y adolescentes. Se estudia la manipulación algorítmica como posible vicio de la voluntad, los dark patterns como herramientas de distorsión del consentimiento y el rol de la arquitectura de elección digital en la formación de contratos electrónicos. Se propone el fortalecimiento de la función notarial como garantía del consentimiento informado en entornos digitales, a la luz del principio "Notary in the Loop" y la jurisprudencia argentina reciente. El trabajo concluye con recomendaciones orientadas a la construcción de un ecosistema digital más justo, accesible y respetuoso de los derechos humanos.

Ponencias

Primera: La vulnerabilidad digital es una categoría jurídica autónoma que requiere reconocimiento normativo expreso en el derecho argentino del consumidor. El consumidor electrónico hipervulnerable merece una protección diferenciada y reforzada que no puede inferirse únicamente de las normas generales del sistema tuitivo vigente. Se recomienda la sanción de una ley específica sobre protección de consumidores electrónicos hipervulnerables que establezca estándares mínimos de accesibilidad, información y seguridad adaptados a las necesidades de cada colectivo.

Segunda: La manipulación algorítmica y los *dark patterns* constituyen prácticas que pueden viciar el consentimiento en la contratación electrónica y que deben ser abordadas mediante una regulación específica que prohíba su uso y establezca responsabilidades claras para los proveedores que los implementen. El derecho argentino dispone de herramientas normativas generales que los operadores jurídicos deben aplicar con criterio teleológico y actualizado, pero la seguridad jurídica requiere una tipificación legal específica de estas prácticas.

Tercera: La economía de datos exige una reforma integral de la Ley 25.326 de Protección de los Datos Personales que incorpore estándares equivalentes al Reglamento General de Protección de Datos europeo: consentimiento granular, portabilidad de datos, derecho a la explicación de decisiones automatizadas, evaluaciones de impacto sobre los derechos y una autoridad de control con recursos y atribuciones suficientes para supervisar efectivamente el tratamiento de datos en entornos de inteligencia artificial. Esta reforma es especialmente urgente para la protección de los consumidores hipervulnerables, quienes son los más expuestos a las consecuencias del perfilamiento algorítmico.

Cuarta: Argentina debe desarrollar un marco regulatorio para la inteligencia artificial que tome como referencia el AI Act europeo, incorporando la clasificación de sistemas de IA por niveles de riesgo, la prohibición de los sistemas que explotan vulnerabilidades de grupos específicos y los requisitos de transparencia y supervisión humana para los sistemas de alto riesgo. Este marco debe articularse con el sistema de protección del consumidor y con la legislación de datos personales para construir una respuesta integral a los desafíos del ecosistema digital.

Quinta: Los entornos de contratación digital presentan características que desafían las presunciones sobre las que se construyó la protección clásica del consumidor: (i) saturación informativa que torna ilusoria la lectura efectiva de términos y condiciones; (ii) arquitecturas de interfaces deliberadamente diseñadas para dificultar la opción de rechazo; (iii) contratos de adhesión donde la voluntad se expresa únicamente como aceptación o exclusión. La intervención de un tercero profesional independiente, dotado de competencia técnico-jurídica y legitimidad institucional, que certifique la libertad, comprensión e información del consentimiento, constituye mecanismo de garantía relevante para el consumidor hipervulnerable. El notariado latino, por su función fedataria y asesora, es institucionalmente apto para desempeñar este rol. La aplicación del principio "Notary in the Loop" (CNUE, 2025) podría operar en transacciones de especial impacto (crédito, seguros, inversión) celebradas por consumidores hipervulnerables, sin implicar burocratización de toda transacción digital.

Índice

I. Introducción

La irrupción de las plataformas digitales en la vida cotidiana ha transformado de manera radical las estructuras de contratación, el ejercicio de la autonomía de la voluntad y las condiciones en que los sujetos participan en el mercado. En el espacio digital, millones de personas celebran contratos, adquieren bienes y servicios, brindan consentimiento a políticas de privacidad y ceden datos personales sin ser plenamente conscientes de las implicancias jurídicas de tales actos. Esta realidad no es neutral, lejos de constituir un escenario de igualdad formal, el entorno digital reproduce y amplifica asimetrías estructurales preexistentes, generando nuevas formas de vulnerabilidad (Salierno, 2024) que el derecho del consumidor no puede ignorar.

La vulnerabilidad, como categoría jurídica y filosófica, no es una condición excepcional sino una dimensión constitutiva de la experiencia humana. Tal como lo señaló la jurista norteamericana Martha Fineman (2008), el sujeto vulnerable no es una anomalía del sistema sino el punto de partida desde el cual debe construirse toda política de igualdad sustantiva. Esta perspectiva resulta especialmente pertinente cuando se trata de consumidores que operan en entornos digitales. La brecha tecnológica, la opacidad algorítmica, la velocidad de los procesos de contratación y la sofisticación de las técnicas persuasivas generan condiciones objetivas de desigualdad que justifican una protección jurídica reforzada.

El consumidor electrónico hipervulnerable es aquel que, además de las asimetrías informativas y económicas propias de toda relación de consumo, enfrenta obstáculos adicionales derivados de su condición personal, edad avanzada, discapacidad, situación socioeconómica precaria, o pertenencia a colectivos históricamente marginados del acceso a la tecnología. Frente a sistemas de inteligencia artificial que predicen comportamientos, plataformas que diseñan interfaces para maximizar la extracción de datos y contratos de adhesión que hacen del *clic* la única forma de expresión de la voluntad, estos sujetos se encuentran en una posición de especial fragilidad que reclama una respuesta normativa adecuada.

El presente trabajo aborda esta problemática desde una perspectiva plural y crítica. Se analiza el marco jurídico argentino vigente, con especial referencia al Código Civil y Comercial de la Nación (Ley 26.994, 2015) y a la Ley de Defensa del

Consumidor (Ley 24.240, 1993), así como el derecho comparado europeo, en particular el Reglamento de Inteligencia Artificial (UE) 2024/1689 y la *Digital Services Act*. Se examina la jurisprudencia argentina reciente sobre consumidores hipervulnerables y se propone la función notarial como garantía institucional del consentimiento informado en la era digital. La protección del consumidor electrónico hipervulnerable no es solo una cuestión de técnica jurídica sino una exigencia ética y de derechos humanos que interpela al ordenamiento jurídico en su conjunto.

Sostenemos que la categoría de vulnerabilidad digital debe ser reconocida normativamente como forma agravada de vulnerabilidad del consumidor, y que la función notarial, reformulada bajo el principio *Notary in the Loop*, puede operar como mecanismo institucional de garantía del consentimiento informado en la contratación electrónica de consumidores hipervulnerables.

Desde el punto de vista metodológico, el trabajo adopta un enfoque interdisciplinario que combina la dogmática jurídica con aportes de la psicología cognitiva, la filosofía moral y los estudios críticos de tecnología. Esta perspectiva interdisciplinaria no es un capricho académico sino una necesidad metodológica ya que la comprensión adecuada de la manipulación algorítmica, la economía de datos y la hipervulnerabilidad digital requiere herramientas conceptuales que exceden los límites de la ciencia jurídica tradicional. Sólo desde una perspectiva integradora es posible hacer justicia a la complejidad del fenómeno y proponer respuestas normativas que sean a la vez técnicamente sólidas y socialmente adecuadas.

II. Desarrollo

1. La vulnerabilidad como categoría jurídica: del sujeto abstracto al sujeto real

El modelo clásico del derecho moderno, heredero de la tradición iusnaturalista y codificado en las grandes sistematizaciones del siglo XIX, construyó su arquitectura sobre la figura del sujeto racional, autónomo y formalmente capaz de ejercer derechos. Esta abstracción, funcional para la configuración de sistemas de igualdad formal, ha revelado progresivamente su insuficiencia para capturar la complejidad de las condiciones materiales en que los sujetos concretos participan en las relaciones jurídicas[1]. La propuesta de Fineman (2008) introduce una reformulación radical:

[1] Kemelmajer de Carlucci, A., "Las personas vulnerables en el derecho privado", *RDPyC*, 2018-3, p. 17.

anclar la igualdad sustantiva en la vulnerabilidad universal como dato ontológico, desplazando el foco desde la excepción hacia el reconocimiento de la vulnerabilidad como condición constitutiva de la experiencia humana[2].

El concepto de vulnerabilidad ha irrumpido en el discurso jurídico contemporáneo como un correctivo necesario a esta abstracción. Fineman (2008) propone reemplazar la noción de "igualdad formal" por la de "igualdad sustantiva", tomando como punto de partida la vulnerabilidad universal del ser humano. Para esta autora, la vulnerabilidad no es una debilidad individual sino una condición compartida que el Estado tiene el deber de atender mediante políticas activas de inclusión y protección. Este enfoque resulta particularmente iluminador para el análisis del derecho del consumidor en entornos digitales, donde las asimetrías no son meramente económicas sino también tecnológicas, cognitivas y psicológicas.

La propuesta de Fineman implica una reformulación radical del sujeto del derecho. Ya no se trata del individuo abstracto del liberalismo clásico (propietario, racional, autosuficiente) sino del ser humano concreto, encarnado en un cuerpo, situado en relaciones sociales de dependencia mutua, expuesto a los vaivenes de la enfermedad, el envejecimiento, la pérdida de capacidades y la precariedad económica. Esta reconceptualización tiene consecuencias prácticas inmediatas para el derecho del consumidor en el entorno digital. Si la vulnerabilidad es la condición normal y no la excepción, el sistema normativo debe construirse desde esa premisa y no como un conjunto de excepciones al modelo del sujeto autónomo.

En el plano normativo argentino, la vulnerabilidad del consumidor fue reconocida tempranamente por la Ley 24.240 de Defensa del Consumidor (1993) y reforzada luego por el Código Civil y Comercial de la Nación (Ley 26.994), cuyo artículo 1094 establece que las normas que regulan las relaciones de consumo deben ser interpretadas conforme al principio de protección del consumidor y al acceso al consumo sustentable. Más específicamente, el artículo 1095 CCCN reconoce que el contrato de consumo debe ser interpretado en el sentido más favorable al consumidor. Estas disposiciones constituyen la expresión normativa de un principio más general,

[2] Fineman, M. A., "The Vulnerable Subject: Anchoring Equality in the Human Condition", *Yale Journal of Law & Feminism*, 20(1), 2008, pp. 1-23.

el principio *pro consumatore*, que orienta la interpretación y la integración de todo el sistema de protección.

Esta tutela reforzada se fundamenta en una asimetría estructural que el propio legislador ha reconocido explícitamente. El proveedor es un operador profesional, con conocimiento técnico, poder económico y acceso a recursos de todo tipo, mientras que el consumidor es un sujeto lego que actúa en un plano de inferioridad objetiva. En el entorno digital, esta asimetría se agudiza exponencialmente ya que las plataformas tecnológicas disponen de sistemas de inteligencia artificial, equipos de expertos en psicología cognitiva y del comportamiento, datos masivos y arquitecturas de elección diseñadas para maximizar la extracción de valor del consumidor. Frente a esta maquinaria sofisticada, el usuario promedio se encuentra en una situación de vulnerabilidad que excede lo meramente informativo y alcanza dimensiones cognitivas, emocionales y conductuales que los esquemas clásicos del derecho no contemplan adecuadamente.

El ordenamiento jurídico reconoce que la igualdad formal es insuficiente cuando las condiciones materiales de los sujetos son radicalmente distintas. De este modo, la vulnerabilidad deja de ser un dato empírico extrajurídico para convertirse en una categoría normativa que activa mecanismos de protección específicos y diferenciados.

1.1. El contexto de la digitalización: brechas, accesos y desigualdades estructurales

Cualquier análisis jurídico sobre la protección del consumidor electrónico en Argentina que pretenda ser socialmente relevante debe partir de una lectura honesta del contexto socioeconómico en que se desarrollan las relaciones de consumo digital. Argentina es un país con altos niveles de penetración de internet, superior al 90% de la población, según los últimos datos disponibles[3], pero con profundas desigualdades en la calidad del acceso, en la alfabetización digital y en la capacidad de ejercer derechos en el entorno digital. La brecha digital no es solo una brecha tecnológica sino una brecha social, educativa y económica que reproduce y amplifica las desigualdades preexistentes en el espacio físico[4].

[3] Instituto Nacional de Estadísticas y Censos informe 2025. Recuperado de https://www.indec.gob.ar/indec/web/Nivel3-Tema-4-26

[4] Observatorio de Desarrollo Digital, CEPAL, ONU. Recuperado de https://desarrollodigital.cepal.org/es/datos-y-hechos/brechas-de-conectividad-como-factor-de-exclusion

Los adultos mayores, las personas con discapacidad, los habitantes de zonas rurales y periurbanas, las personas en situación de pobreza y las poblaciones indígenas tienen accesos radicalmente distintos a las infraestructuras digitales, a los dispositivos tecnológicos y a las competencias necesarias para navegar con seguridad y autonomía en el entorno en línea. Esta realidad tiene consecuencias directas para el derecho del consumidor. Estamos frente a un sistema de protección que asume que todos los consumidores tienen acceso a internet de alta velocidad, dispositivos modernos y competencias digitales avanzadas construido sobre una ficción que excluye a los segmentos más vulnerables de la población.

La pandemia de COVID-19 aceleró de manera drástica la digitalización de las relaciones de consumo en Argentina. Servicios que antes podían accederse de manera presencial como trámites bancarios, renovación de documentos, consultas médicas, acceso a prestaciones de la seguridad social, migraron de manera acelerada al entorno digital, muchas veces sin los necesarios períodos de transición, sin estrategias de inclusión para los colectivos vulnerables y sin la formación adecuada para los propios agentes públicos. El resultado fue una exclusión sistemática de los consumidores más vulnerables de servicios esenciales, que fueron forzados a interactuar con interfaces digitales para las que no estaban preparados o a depender de intermediarios como familiares, vecinos o gestores, con los riesgos de fraude y abuso que ello implica.

Esta realidad estructural impone una obligación adicional a los proveedores de servicios digitales que se cristaliza en la obligación de garantizar que sus plataformas sean accesibles y utilizables por todos los segmentos de la población, incluyendo los que tienen menor familiaridad con la tecnología. El *principio de diseño universal*, incorporado al derecho argentino a través de la Convención sobre los Derechos de las Personas con Discapacidad (CDPD)[5], exige que los productos y servicios sean concebidos desde el inicio para ser utilizables por el mayor número posible de personas, sin necesidad de adaptaciones ni diseños especializados. En el contexto de la contratación electrónica, este principio implica que las interfaces, los procesos

[5] Convención sobre los Derechos de las Personas con Discapacidad https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf

de registro y aceptación, y los mecanismos de resolución de conflictos deben ser diseñados pensando en el usuario más vulnerable y no en el usuario más capaz.

La inclusión financiera digital, uno de los objetivos declarados de las políticas públicas argentinas de los últimos años, ofrece un ejemplo paradigmático de esta tensión. Las billeteras virtuales, el crédito en línea y los servicios de pago digital han ampliado significativamente el acceso de poblaciones antes excluidas del sistema financiero formal. Pero al mismo tiempo han creado nuevas formas de exclusión y vulnerabilidad; personas mayores que no comprenden los mecanismos de seguridad de sus cuentas digitales, trabajadores informales que acceden a créditos de altas tasas de interés mediante interfaces diseñadas para facilitar la aceptación y dificultar la lectura de las condiciones, jóvenes que acumulan deudas en plataformas de juego y entretenimiento que explotan su impulsividad y su deseo de pertenencia social. La inclusión digital sin protección digital adecuada no es una política de derechos sino una política de mercado.

2. El consumidor electrónico hipervulnerable

Si la vulnerabilidad del consumidor es la regla en el entorno digital, la hipervulnerabilidad designa aquellas situaciones en que dicha vulnerabilidad alcanza su nivel más crítico. El consumidor electrónico hipervulnerable es aquel que, sobre la base de la asimetría estructural propia de toda relación de consumo, enfrenta factores adicionales, ya sea personales, sociales, económicos o tecnológicos, que intensifican la brecha, su situación de desventaja y exigen una respuesta jurídica diferenciada.

La doctrina y la jurisprudencia argentina han identificado tres grandes colectivos de consumidores hipervulnerables en el entorno digital: los adultos mayores, las personas con discapacidad y los niños y adolescentes. Cada uno de estos grupos enfrenta vulnerabilidades específicas que merecen ser analizadas con detenimiento.

2.1 Adultos mayores

Los adultos mayores constituyen uno de los colectivos más expuestos a la victimización en entornos digitales. La combinación de menor familiaridad con las tecnologías de la información y la comunicación, menor capacidad crítica frente a interfaces diseñadas para confundir, y mayor propensión a la confianza interpersonal, los convierte en blanco preferencial de fraudes digitales, manipulación algorítmica y abuso contractual en plataformas electrónicas.

La Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores establece el derecho de las personas mayores a la protección y seguridad en sus relaciones con el sector privado, incluyendo las transacciones comerciales. Este instrumento internacional, de jerarquía constitucional en el sistema jurídico argentino, impone a los estados el deber de adoptar medidas de prevención y protección frente a los abusos que puedan sufrir los adultos mayores en el mercado, incluyendo el mercado digital.

En la jurisprudencia argentina reciente, la Cámara de Apelación de Morón, en la causa MO-30821-2025, resolvió un caso paradigmático de phishing que afectó a un adulto mayor como consumidor hipervulnerable. En esa resolución, el tribunal aplicó los principios de la vulnerabilidad agravada para imponer al banco demandado una responsabilidad objetiva y solidaria, con fundamento en la omisión de medidas de seguridad adecuadas a la condición particular del cliente y en la falta de implementación de protocolos específicos para la detección y prevención de fraudes que afectan a usuarios mayores. La sentencia constituye un hito en la protección del consumidor electrónico hipervulnerable y sienta las bases para una doctrina jurisprudencial que integra la variable etaria como factor calificante de la responsabilidad del proveedor digital.

2.2 Personas con discapacidad

Las personas con discapacidad enfrentan barreras específicas en el acceso y uso de las plataformas digitales. La falta de diseño accesible, la ausencia de formatos alternativos de presentación de la información y la complejidad de los procesos de consentimiento electrónico constituyen obstáculos que limitan gravemente su autonomía en las relaciones de consumo digitales.

La Convención sobre los Derechos de las Personas con Discapacidad establece el derecho a la accesibilidad como un principio transversal que incluye el acceso a la información y a las tecnologías de la comunicación (art. 9). En el plano del derecho del consumidor, este principio se traduce en la obligación de los proveedores de garantizar interfaces accesibles, procesos de contratación adaptados y mecanismos de atención específicos para personas con discapacidad.

La economía de datos plantea riesgos adicionales para este colectivo ya que los algoritmos de perfilamiento pueden identificar y explotar condiciones de discapacidad para aplicar precios diferenciales, ofrecer productos inadecuados o diseñar interfaces que aprovechen sus limitaciones específicas. Estas prácticas

constituyen una forma de discriminación algorítmica que el derecho debe abordar con urgencia.

El modelo social de la discapacidad, que desplaza el foco de las limitaciones individuales hacia las barreras ambientales y sociales que impiden la participación plena, es el paradigma que debe orientar la regulación del comercio electrónico en lo que respecta a las personas con discapacidad. La cuestión no es si la persona puede adaptarse al entorno digital existente, sino si el entorno digital está diseñado para permitir la participación plena de todas las personas, independientemente de sus capacidades. Este reencuadre tiene consecuencias jurídicas directas. En este sentido, la inaccesibilidad de una plataforma digital para personas con discapacidad no es un defecto de la persona sino un incumplimiento del proveedor, que activa las consecuencias del régimen de responsabilidad del consumidor y, potencialmente, del régimen antidiscriminatorio.

2.3 Niños, niñas y adolescentes

Los menores de edad representan un caso paradigmático de hipervulnerabilidad en el entorno digital. La facilidad con que los menores otorgan consentimientos electrónicos, aceptan políticas de privacidad y realizan transacciones comerciales contrasta con su escasa comprensión de los efectos de esos actos.

La neurociencia del desarrollo ha demostrado que el córtex prefrontal, región cerebral responsable de la evaluación de riesgos, la planificación a largo plazo y la resistencia a la influencia social, no alcanza su madurez hasta los veinticinco años aproximadamente. Esta realidad biológica tiene consecuencias jurídicas directas ya que los menores de edad son intrínsecamente más susceptibles a las técnicas de manipulación conductual que explotan la impulsividad, el deseo de pertenencia social y la sensibilidad al refuerzo inmediato. Los diseñadores de plataformas digitales conocen y aprovechan estas vulnerabilidades específicas, construyendo experiencias de usuario que generan adicción, maximizan el tiempo de pantalla y optimizan la extracción de datos y dinero de los usuarios más jóvenes.

El Código Civil y Comercial de la Nación establece el principio del interés superior del niño como eje interpretativo de todo el derecho privado (art. 26 CCCN), lo que debe trasladarse al análisis de las relaciones de consumo digitales que involucran a menores. La Ley 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes refuerza esta protección, imponiendo al Estado y a los operadores privados deberes específicos de cuidado. Sin embargo, la aplicación de

estos principios a las plataformas digitales comerciales sigue siendo incipiente en la jurisprudencia y la práctica administrativa argentina.

En el plano europeo, el Reglamento General de Protección de Datos (RGPD) establece en su artículo 8 que el tratamiento de datos de menores de 16 años (13 años según la legislación nacional de cada estado miembro) requiere el consentimiento de los padres o tutores. Esta norma, en combinación con la *Digital Services Act,* ha sentado las bases para una protección reforzada de los menores en el entorno digital que el derecho argentino debería incorporar con mayor decisión. La DSA prohíbe expresamente en su artículo 28 la publicidad dirigida a menores de edad basada en perfilamiento, reconociendo que esta práctica constituye una forma de manipulación que afecta el desarrollo autónomo de la personalidad del menor y compromete su capacidad de ejercer derechos en condiciones de libertad real.

3. Deberes de información en la contratación electrónica

El derecho de información del consumidor es uno de los pilares fundamentales del sistema tuitivo construido por la ley de defensa al consumidor y el CCCN. En el entorno digital, este derecho adquiere una dimensión particularmente crítica debido a la velocidad de los procesos de contratación, la extensión de los términos y condiciones, la opacidad de los algoritmos de recomendación y la asimetría cognitiva entre plataformas y usuarios tornan imperativo un análisis riguroso de los deberes informativos en la contratación electrónica.

El artículo 1107 del CCCN establece los requisitos de información previa en los contratos celebrados a distancia y por medios electrónicos. La norma exige que el proveedor informe, de manera clara y comprensible, los datos de identificación del proveedor, las características esenciales del bien o servicio, el precio total, las condiciones de contratación, el derecho de arrepentimiento y los medios técnicos para corregir errores antes de la celebración del contrato. Estos requisitos, que deben entenderse como un piso mínimo indisponible, resultan frecuentemente incumplidos o satisfechos de manera meramente formal mediante políticas de privacidad y términos y condiciones extensos, escritos en lenguaje técnico inaccesible para el usuario promedio.

El fenómeno conocido como "fatiga del consentimiento" (estudiado extensamente por la investigación en psicología cognitiva y comportamiento del consumidor) ilustra de manera contundente la insuficiencia del paradigma informativo clásico para la era digital. Los estudios demuestran que los usuarios promedio se

encontrarían leyendo políticas de privacidad durante semanas al año si leyeran efectivamente todos los documentos que firman digitalmente. Ante la imposibilidad práctica de cumplir este deber de lectura, los consumidores adoptan una postura de confianza ciega o de aceptación acrítica que vacía de contenido real el consentimiento informado. Esta situación es especialmente grave para los consumidores hipervulnerables, quienes presentan mayores dificultades para navegar por interfaces complejas y para comprender documentos redactados en lenguaje técnico-jurídico.

El cumplimiento del deber de información adquiere una relevancia especial respecto de los consumidores hipervulnerables. Los adultos mayores con menor alfabetización digital, las personas con discapacidad visual o cognitiva y los menores de edad requieren formatos informativos adaptados a sus condiciones específicas. El principio de diseño universal aplicado a la contratación electrónica impone a los proveedores la obligación de garantizar que la información sea accesible y comprensible para todos los segmentos de la población, no solo para el usuario estándar. Esto implica, entre otras cosas, el uso de lenguaje simple, la provisión de formatos alternativos (audio, pictogramas, videos de lenguaje de señas), la compatibilidad con tecnologías asistivas y el diseño de interfaces que guíen activamente al usuario hacia la información más relevante.

La dimensión temporal del deber de información también merece consideración. El artículo 1107 CCCN exige que la información sea proporcionada de manera previa y en la oportunidad adecuada para que el consumidor pueda tomar una decisión informada. En la práctica de la contratación electrónica, sin embargo, la información más relevante (incluyendo los costos totales, las condiciones de cancelación y los términos del tratamiento de datos personales) suele aparecer en las etapas finales del proceso de contratación, cuando el consumidor ya ha invertido tiempo y energía en el proceso y está psicológicamente comprometido con la conclusión del acuerdo. Esta práctica, conocida como el efecto de inversión o costo irrecuperable aplicado al diseño de interfaces, constituye una forma de manipulación conductual que compromete la libertad real del consentimiento.

La información sobre el tratamiento de datos personales merece una mención especial. La Ley 25.326 de Protección de los Datos Personales establece el derecho del titular a ser informado sobre la finalidad del tratamiento, los destinatarios de los datos y los derechos de acceso, rectificación, supresión y bloqueo. En el entorno digital, el cumplimiento de estos derechos está frecuentemente subordinado a

procesos complejos, formularios inaccesibles y plazos prolongados que hacen ilusorio el ejercicio efectivo del control sobre los propios datos. La reforma de esta ley en clave de los estándares del RGPD europeo, con especial atención a las necesidades de los consumidores hipervulnerables, constituye una prioridad ineludible de la agenda legislativa argentina.

4. Contratos de adhesión y consentimiento por clic. El derecho de arrepentimiento

La contratación electrónica se caracteriza por la celebración de contratos de adhesión cuyas cláusulas son predispuestas unilateralmente por el proveedor y presentadas al consumidor como un bloque inmodificable: o las acepta en su totalidad o no accede al servicio. Esta estructura contractual, que el CCCN regula en sus artículos 984 a 989, alcanza en el entorno digital una expresión particularmente extrema: el consumidor no solo no puede negociar las cláusulas, sino que frecuentemente ni siquiera las ha leído ni está en condiciones de comprenderlas.

El consentimiento electrónico expresado mediante un clic denominado *"clickwrap agreement"* plantea serios interrogantes sobre la validez del consentimiento informado como elemento esencial del acto jurídico. El artículo 1106 del CCCN reconoce la validez de los contratos celebrados por medios electrónicos, pero esta validez no puede disociarse de los requisitos sustanciales del consentimiento: libertad, información, comprensión y ausencia de vicios. Cuando un consumidor acepta términos y condiciones de treinta páginas haciendo clic en un botón sin haber leído el documento, el consentimiento formalmente expresado puede estar viciado en su sustancia.

La doctrina y la jurisprudencia han desarrollado criterios para la interpretación de estos contratos. El artículo 988 CCCN establece la nulidad de las cláusulas que desnaturalizan las obligaciones del predisponente, implican renuncia o restricción de derechos del adherente, o son abusivas en los términos del artículo 1119 CCCN. El artículo 1117 CCCN complementa estas reglas para los contratos de consumo, estableciendo que las cláusulas abusivas son nulas de pleno derecho.

El derecho de arrepentimiento, reconocido en el artículo 1110 del CCCN, es una herramienta fundamental en la protección del consumidor en la contratación a distancia. Esta norma otorga al consumidor el derecho a revocar la aceptación dentro del plazo de diez días corridos desde la celebración del contrato o desde la recepción del bien, sin necesidad de expresar causa y sin costo alguno. El ejercicio de este

derecho no puede ser restringido por cláusulas predispuestas, y cualquier renuncia anticipada al mismo carece de efectos jurídicos.

Sin embargo, la operatividad práctica del derecho de arrepentimiento está frecuentemente obstaculizada por el diseño de las plataformas. Procesos complejos de cancelación, ausencia de botones visibles de renuncia, formularios con múltiples pasos y plazos artificialmente reducidos son algunas de las técnicas empleadas por los proveedores para desincentivar el ejercicio de este derecho. Estas prácticas, que serán analizadas más extensamente en el apartado sobre *dark patterns*, constituyen formas de manipulación conductual que comprometen la validez del consentimiento y la efectividad del sistema de protección.

5. La manipulación algorítmica: *dark patterns,* arquitecturas de elección y asimetrías cognitivas

Uno de los desarrollos más relevantes y perturbadores del derecho digital contemporáneo es el reconocimiento de que los algoritmos no son herramientas neutrales de intermediación sino sistemas activos de influencia sobre el comportamiento humano. Las plataformas digitales disponen de sofisticados mecanismos de diseño de interfaces conocidos como *dark patterns* o patrones oscuros que explotan sesgos cognitivos, vulnerabilidades emocionales y mecanismos psicológicos inconscientes para inducir al consumidor a tomar decisiones que no responden a su voluntad libre e informada.

Desde la perspectiva del derecho civil clásico, los *dark patterns* plantean interrogantes fundamentales respecto a la naturaleza del consentimiento. Mientras la teoría tradicional vincula los vicios de la voluntad (error, dolo, intimidación) a defectos en la cognición o intención del sujeto (art. 265 CCCN), los *dark patterns* operan mediante distorsión del contexto de decisión, no del sujeto per se. Es, por tanto, más preciso caracterizarlos como violaciones al deber de información (art. 1100 CCCN) y al principio de buena fe (arts. 9 y 961 CCCN), encuadrándolos dogmáticamente en el régimen de cláusulas abusivas (art. 988 CCCN y art. 37 Ley 24.240) antes que en el de vicios clásicos de la voluntad[6]. Esta operación hermenéutica permite proteger al consumidor sin forzar categorías que presuponen defectos subjetivos.

[6] Barocelli, S. S., "Hacia la construcción de la categoría de consumidores hipervulnerables", *La Ley*, 2018-F, 929; Hernández, C. A. - Frustagli, S., "Hipervulnerabilidad y prácticas abusivas", *RDCO*, 2017-B, 145.

Los *dark patterns* fueron inicialmente identificados por el diseñador de experiencia de usuario Harry Brignull[7], y desde entonces han sido objeto de creciente atención regulatoria y académica. Se trata de técnicas de diseño de interfaces que deliberadamente confunden, distraen o manipulan al usuario para obtener resultados que benefician al proveedor en detrimento del consumidor. Algunos ejemplos paradigmáticos incluyen: las *"roach motels"* (suscripciones fáciles de contratar pero difíciles de cancelar), el *"confirmshaming"* (opciones de rechazo formuladas de manera culpabilizante), el "*misdirection"* (desvío de la atención visual hacia la opción preferida por el proveedor), los *"hidden costs"* (cargos adicionales revelados solo en la última etapa del proceso de compra) y los *"trick questions"* (preguntas formuladas de manera ambigua para obtener consentimientos no deseados).

La relevancia jurídica de estas prácticas reside en su potencial para configurar un vicio de la voluntad en los términos del derecho civil clásico. La noción de "arquitectura de elección", desarrollada por Sunstein y Thaler (2008) en el marco de la teoría del *nudge*[8]*,* proporciona un instrumental conceptual valioso para el análisis jurídico de estas prácticas. El arquitecto de elección es quien diseña el entorno en que las personas toman sus decisiones. La disposición de los elementos en una pantalla, el orden de las opciones, los colores empleados y los mensajes de refuerzo son todos factores que influyen de manera significativa sobre las elecciones del usuario. Sunstein (2013) advierte que estas técnicas pueden ser empleadas tanto para facilitar elecciones racionales como para explotar las debilidades cognitivas humanas, y propone criterios normativos para distinguir los *nudges* legítimos de los manipuladores.

Las asimetrías cognitivas son otro factor crítico en el análisis de la contratación electrónica. Los sistemas de inteligencia artificial disponen de un conocimiento exhaustivo de los sesgos cognitivos del usuario obtenido a través del análisis masivo de datos de comportamiento y los explotan sistemáticamente para maximizar la extracción de valor. Harari (2016) señala que en la era del *big data* los algoritmos

[7] https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf

[8] https://www.researchgate.net/publication/235413094_NUDGE_Improving_Decisions_About_Health_Wealth_and_Happiness

conocen al sujeto mejor de lo que el sujeto se conoce a sí mismo, lo que plantea una asimetría radical que socava los fundamentos mismos de la autonomía individual.

El derecho argentino no cuenta aún con una regulación específica sobre *dark patterns,* pero los principios generales del derecho del consumidor y del derecho civil proporcionan herramientas suficientes para abordar estas prácticas. La cláusula general de buena fe (art. 9 CCCN), la prohibición de las cláusulas abusivas (art. 988 CCCN), el deber de información (art. 1107 CCCN) y la tutela contra los vicios de la voluntad (arts. 265 a 278 CCCN) constituyen una base normativa que los operadores jurídicos deben aplicar con criterio teleológico y actualizado a las realidades del entorno digital. En el plano comparado, la *Digital Services Act* europea (Reglamento UE 2022/2065) prohíbe expresamente los *dark patterns* en sus artículos 25 y 26, estableciendo que los proveedores de plataformas en línea no pueden utilizar interfaces de usuario que de alguna manera engañen, manipulen o perjudiquen a los destinatarios del servicio, ni que les dificulten tomar decisiones autónomas e informadas. Esta regulación constituye un modelo de referencia para el desarrollo del derecho argentino en la materia.

Corvalán (2018) ha señalado que los algoritmos de inteligencia artificial plantean desafíos inéditos para el derecho, en particular en lo que se refiere a la atribución de responsabilidad por las decisiones adoptadas de manera autónoma por sistemas automatizados. En el contexto de la contratación electrónica, esta reflexión adquiere particular relevancia. Cuando un sistema de IA diseña una arquitectura de elección específicamente orientada a explotar las vulnerabilidades cognitivas de un consumidor hipervulnerable, la responsabilidad del proveedor que lo despliega debe ser evaluada con criterios de objetividad y de prevención que trasciendan los esquemas clásicos de culpa y dolo.

6. La economía de datos: recolección, perfilamiento y predicción de comportamiento

La arquitectura económica de las plataformas digitales descansa en la extracción sistemática y el procesamiento de datos personales como insumo central de rentabilidad[9]. Harari (2016) caracterizó esta transformación como "dataísmo", pero

[9] Zuboff, S., *The Age of Surveillance Capitalism*, PublicAffairs, 2019, pp. 63-97; Picasso, S., "Las responsabilidades en la contratación electrónica", *RDC*, 2022-A, 45.

una teorización más aguda proviene de Zuboff (2019), quien documenta la emergencia de un "capitalismo de vigilancia" que convierte la experiencia humana en materia prima para "productos predictivos" destinados al mercado de futuros comportamentales. Para los consumidores hipervulnerables, esta dinámica genera capas adicionales de riesgo: a las asimetrías informativas clásicas se suman las relativas a recolección, procesamiento y uso predictivo de datos para manipular su comportamiento. La Ley 25.326, aun reconociendo derechos fundamentales (acceso, rectificación, supresión), descansa en la presunción de que los titulares pueden ejercer control racional y eficaz sobre sus datos, presunción particularmente frágil frente a sujetos de edad avanzada, educación limitada o capacidades cognitivas diferentes.

La Ley 25.326 de Protección de los Datos Personales establece principios fundamentales para el tratamiento de datos personales: finalidad determinada, proporcionalidad, consentimiento informado y derecho de oposición. Sin embargo, la normativa argentina muestra sus limitaciones frente a la complejidad de los sistemas de tratamiento de datos contemporáneos: el concepto de "consentimiento informado" resulta insuficiente cuando la finalidad real del tratamiento es inaccesible para el usuario y cuando los efectos del perfilamiento se proyectan sobre todas las dimensiones de su vida.

La Resolución 139/2020 del SIGEN[10] representó un avance significativo en la regulación del tratamiento de datos en el sector público, estableciendo criterios de seguridad y minimización de datos que debieran extenderse al sector privado. La experiencia comparada, en particular el Reglamento General de Protección de Datos de la Unión Europea, demuestra que es posible construir un marco normativo más robusto que garantice el control efectivo de los ciudadanos sobre sus datos personales.

El Reglamento de Inteligencia Artificial de la Unión Europea (UE) 2024/1689 introduce una clasificación de los sistemas de IA por niveles de riesgo que resulta especialmente relevante para la protección del consumidor hipervulnerable. El Reglamento prohíbe los sistemas de IA que explotan las vulnerabilidades específicas de grupos de personas debido a su edad, discapacidad u otras circunstancias para

[10] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-139-2020-338055/texto

distorsionar su comportamiento de manera que les cause o pueda causar perjuicios físicos, psicológicos o económicos. Esta prohibición, que constituye un límite absoluto no susceptible de derogación por las partes, es directamente aplicable a los sistemas de perfilamiento y manipulación conductual que afectan a consumidores hipervulnerables.

El derecho argentino debe avanzar en una dirección similar. La combinación de una reforma de la Ley 25.326 que incorpore los estándares del RGPD europeo con la regulación específica de los sistemas de inteligencia artificial de alto riesgo constituiría un paso fundamental hacia la construcción de un ecosistema digital que respete la dignidad y la autonomía de los consumidores, y especialmente de los más vulnerables.

7. Jurisprudencia: el caso de phishing contra adultos mayores

La jurisprudencia argentina ha comenzado a desarrollar una doctrina específica sobre la protección de los consumidores hipervulnerables en el entorno digital, que merece ser analizada con detenimiento por su relevancia práctica y por su capacidad para iluminar las respuestas del derecho vigente a los nuevos desafíos tecnológicos.

El phishing es técnica de fraude que consiste en suplantar la identidad de entidades confiables para obtener credenciales bancarias u otro tipo de información sensible. Es uno de los fenómenos más extendidos de victimización digital y afecta de manera desproporcionada a los adultos mayores.

La combinación de menor alfabetización digital, mayor confianza interpersonal y menor familiaridad con los protocolos de seguridad hace de este colectivo el blanco preferencial de estas modalidades delictivas. Los datos estadísticos disponibles confirman que los adultos mayores de sesenta y cinco años representan una proporción desproporcionadamente alta de las víctimas de fraudes digitales en Argentina y en el mundo, con pérdidas económicas que en muchos casos resultan irreparables dado que afectan los ahorros de toda una vida.

La Cámara de Apelación de Morón, en la causa MO-30821-2025[11], abordó un caso paradigmático en el que un adulto mayor fue víctima de una operación de

[11] Cámara de Apelación de Morón. (2025). “PEA c/ BDLPDBA y otros s/ medida cautelar”, la Sala II de la Cámara Civil y Comercial de Morón, *Causa MO-30821-2025*. Resolución judicial sobre phishing y consumidor hipervulnerable. Poder Judicial de la Provincia de Buenos Aires. https://www.diariojudicial.com/news-102261-hipervulnerable-hiperprotegido

phishing que resultó en la sustracción de sus fondos bancarios. Los hechos del caso presentaban las características típicas de este tipo de fraude: el consumidor recibió un mensaje de texto que simulaba ser enviado por su entidad bancaria, con un hipervínculo que lo redirigió a un sitio web fraudulento que imitaba la apariencia del portal oficial del banco, donde proporcionó sus credenciales de acceso y su código de seguridad. Con esos datos, los autores del fraude realizaron transferencias no autorizadas por montos significativos.

El tribunal, aplicando los principios del sistema de responsabilidad objetiva del proveedor en las relaciones de consumo (arts. 40 y 40 bis de la Ley 24.240) y el estándar reforzado de diligencia exigible a las entidades financieras en su condición de proveedores de servicios esenciales, concluyó que el banco había incurrido en responsabilidad al no implementar mecanismos de detección y alerta específicos para operaciones que presentaban características propias del fraude, y al no haber adoptado medidas de diligencia especial respecto de un cliente cuya edad y perfil transaccional hacían previsible una mayor exposición al riesgo. La sentencia rechazó el argumento del banco en el sentido de que la responsabilidad era exclusiva del consumidor por haber proporcionado sus credenciales, señalando que este razonamiento ignora la naturaleza misma del phishing como técnica de ingeniería social específicamente diseñada para superar las defensas cognitivas del usuario promedio, y especialmente de los usuarios pertenecientes a grupos vulnerables.

La sentencia es importante por varios motivos. En primer lugar, aplica el concepto de consumidor hipervulnerable para elevar el estándar de diligencia exigible al proveedor. En este aspecto, no basta con cumplir las medidas de seguridad estándar cuando el proveedor conoce o debería conocer que el cliente pertenece a un colectivo especialmente expuesto a determinados tipos de fraude. Las entidades financieras, que disponen de datos exhaustivos sobre el perfil y el comportamiento de sus clientes, están en condiciones de identificar a los usuarios adultos mayores y de implementar protocolos específicos de alertas, doble verificación y acompañamiento personalizado. La omisión de estas medidas, cuando el riesgo era previsible, configura una culpa in vigilando que compromete la responsabilidad del proveedor.

En segundo lugar, la sentencia establece un vínculo directo entre la omisión de medidas preventivas específicas y la responsabilidad por el daño sufrido, configurando un supuesto de responsabilidad por omisión en el marco de la prestación de servicios digitales. En tercer lugar, la resolución integra la perspectiva

de los derechos humanos de las personas mayores con referencia explícita a la CIDHPM en el análisis de las obligaciones de los proveedores de servicios financieros digitales, abriendo un camino para la articulación entre el derecho del consumidor y el derecho internacional de los derechos humanos en el tratamiento de la hipervulnerabilidad.

Esta jurisprudencia sienta las bases para una doctrina más amplia que debería extenderse a otros contextos de vulnerabilidad digital: plataformas de comercio electrónico que no implementan mecanismos de verificación de identidad adecuados para adultos mayores, aplicaciones de servicios financieros diseñadas sin consideración de las necesidades de accesibilidad de las personas con discapacidad, y plataformas de entretenimiento digital que explotan las vulnerabilidades psicológicas de los menores de edad. El principio subyacente es claro: quien diseña y opera un sistema digital que es utilizado por consumidores hipervulnerables asume una obligación de seguridad y de diligencia reforzada que no puede ser transferida al usuario mediante cláusulas de exoneración de responsabilidad en los términos y condiciones del servicio.

8. El Reglamento Europeo de Inteligencia Artificial (AI Act) y la Digital Services Act como marcos regulatorios comparados

La Unión Europea ha liderado el desarrollo de marcos regulatorios para la economía digital que constituyen referencias ineludibles para el análisis del derecho argentino. El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (AI Act) y la Digital Services Act (Reglamento UE 2022/2065) representan los dos pilares de una arquitectura regulatoria orientada a garantizar que la inteligencia artificial y las plataformas digitales sirvan a los seres humanos en lugar de explotarlos.

El AI Act establece un sistema de clasificación de los sistemas de IA por niveles de riesgo: riesgo inaceptable (prohibido), alto riesgo (regulado), limitado riesgo (sujeto a obligaciones de transparencia) y mínimo riesgo (no regulado). En la categoría de riesgo inaceptable, el Reglamento incluye expresamente las técnicas de manipulación subliminal, la explotación de vulnerabilidades de grupos específicos y los sistemas de calificación social por parte de autoridades públicas. Para los sistemas de IA de alto riesgo, entre los que se incluyen los empleados en la evaluación de crédito, la contratación laboral y la educación, el Reglamento impone requisitos exigentes de transparencia, documentación, supervisión humana y registro en bases de datos públicas. La relevancia del AI Act para la protección del consumidor hipervulnerable

es múltiple. En primer lugar, prohíbe los sistemas de IA que explotan vulnerabilidades específicas de grupos poblacionales para distorsionar su comportamiento, lo que incluye directamente a los algoritmos de perfilamiento y manipulación conductual que afectan a adultos mayores, personas con discapacidad y menores de edad. En segundo lugar, impone requisitos de transparencia que permiten a los consumidores conocer cuándo están interactuando con un sistema de IA y con qué finalidad. En tercer lugar, establece el derecho a una explicación humana de las decisiones automatizadas que afectan de manera significativa a las personas, lo que resulta especialmente relevante para las decisiones de crédito, seguros y otros servicios financieros.

El AI Act introduce además el concepto de "sistemas de IA de propósito general" (GPAI), que incluye los grandes modelos de lenguaje e IA generativa, imponiendo obligaciones específicas de transparencia y evaluación de riesgos a sus desarrolladores. Esta regulación es especialmente relevante para la protección del consumidor hipervulnerable en el contexto de los asistentes virtuales, los *chatbots* de atención al cliente y los sistemas de asesoramiento financiero automatizado, que interactúan directamente con los consumidores más vulnerables y pueden generar confianza indebida o proporcionar información errónea con consecuencias patrimoniales significativas. La exigencia de que estos sistemas sean evaluados y documentados antes de su despliegue en el mercado es un avance regulatorio que Argentina debería adoptar como referencia en el desarrollo de su propio marco para la IA.

La interacción entre el AI Act y la DSA configura un ecosistema regulatorio europeo que establece obligaciones complementarias para las plataformas de gran tamaño. La DSA impone obligaciones de transparencia sobre los algoritmos de recomendación que incluye el derecho del usuario a acceder a una versión del servicio que no utilice perfilamiento y se articulan con las obligaciones de explicabilidad del AI Act para crear un régimen integral de protección frente a la toma de decisiones automatizada.

Esta arquitectura regulatoria, construida sobre el principio de que el ser humano debe mantener el control de las decisiones que le conciernen llamado principio de "*human oversight*" o supervisión humana, es especialmente relevante para la protección de los consumidores hipervulnerables.

La *Digital Services Act,* por su parte, regula las plataformas de intermediación en línea con el objetivo de garantizar un entorno digital seguro y responsable. Entre sus disposiciones más relevantes para la protección del consumidor hipervulnerable se destacan: la prohibición de los *dark patterns* (art. 25), la obligación de transparencia sobre los sistemas de recomendación algorítmica (art. 27), la prohibición de la publicidad dirigida a menores de edad basada en perfilamiento (art. 28) y la obligación de las plataformas de muy gran tamaño de realizar evaluaciones anuales de los riesgos sistémicos que sus sistemas generan, incluyendo los riesgos para los derechos fundamentales (art. 34).

Argentina no cuenta con una legislación equivalente al AI Act ni a la DSA, pero la tendencia regulatoria global apunta en esta dirección. El Consejo de Derechos Humanos de Naciones Unidas ha adoptado resoluciones que vinculan la regulación de la IA con los derechos humanos, y varios estados latinoamericanos, entre ellos Brasil, Chile y Colombia, están avanzando en el desarrollo de marcos regulatorios nacionales para la inteligencia artificial. En este contexto, la experiencia regulatoria europea constituye un laboratorio de relevancia invaluable para el diseño de políticas públicas en materia de protección del consumidor digital en Argentina.

9. La función notarial en la contratación electrónica: garantía del consentimiento informado

La contratación electrónica plantea desafíos fundamentales a la teoría del consentimiento informado como elemento esencial del acto jurídico. La velocidad de los procesos de aceptación, la complejidad de los documentos contractuales, la asimetría de información y el uso de técnicas de persuasión y manipulación hacen que el consentimiento formalmente expresado mediante un *clic* o una firma electrónica pueda estar sustancialmente viciado. En este contexto, la función notarial emerge como una garantía institucional de primer orden para la validez real del consentimiento en las relaciones jurídicas digitales.

Hemos desarrollado extensamente el concepto de notario como garante de los derechos digitales (Salierno-Spina, 2026), argumentando que la función notarial debe adaptarse a las realidades del entorno digital sin perder su naturaleza garantizadora. En este marco, la escritura pública electrónica, la firma electrónica certificada notarialmente y la asesoría notarial previa a la aceptación de contratos de adhesión de especial complejidad o impacto constituyen herramientas de protección del

consumidor hipervulnerable que merecen ser incorporadas al sistema normativo argentino.

El Consejo de Notariados de la Unión Europea (CNUE) ha desarrollado el concepto de "*Notary in the Loop"* (NITL) en su AI Handbook for Notaries (2025) como respuesta a los desafíos que la inteligencia artificial plantea a la función notarial. El principio NITL propone que en los procesos de contratación electrónica mediados por IA que afectan a derechos relevantes, el notario no debe ser desplazado por el sistema automatizado sino mantenerse como garante de la comprensión humana del acto, verificando que el consentimiento expresado sea verdaderamente informado, libre y voluntario. Este principio es especialmente relevante para la protección de los consumidores hipervulnerables, quienes son precisamente los más expuestos a las consecuencias de un consentimiento electrónico formalmente válido pero sustancialmente viciado. La implementación del principio NITL en el derecho argentino y su incorporación al sistema de protección del consumidor electrónico hipervulnerable representaría un avance significativo. Contratos de crédito electrónico, adhesiones a plataformas de inversión digital, *crowfunding*, tokenización inmobiliaria, contratación de seguros en línea y transmisiones de inmuebles mediante herramientas digitales son algunos de los contextos en que la intervención notarial podría garantizar la autenticidad del consentimiento y la protección de los sujetos más vulnerables.

En el plano práctico, la función notarial en la contratación electrónica con consumidores hipervulnerables podría articularse en distintos niveles. En un primer nivel, el notario podría actuar como certificador del proceso de contratación, verificando la identidad de las partes, la integridad del documento contractual y la regularidad del proceso de aceptación. En un segundo nivel, el notario podría asumir una función de asesoramiento previo, explicando al consumidor hipervulnerable el alcance y las consecuencias del contrato que va a celebrar, con las adaptaciones comunicativas necesarias para garantizar la efectividad real del asesoramiento. En un tercer nivel, el notario podría intervenir como garante del consentimiento informado, certificando que el consumidor ha comprendido el acto y lo ha celebrado con plena libertad. Este modelo escalonado permitiría adaptar la intensidad de la intervención notarial a la complejidad e impacto del acto jurídico, sin imponer costos desproporcionados en todas las transacciones del mercado digital.

10. Palabras finales y prospectiva

El sistema normativo argentino de protección del consumidor electrónico hipervulnerable se construye sobre varias capas normativas que merecen ser analizadas de manera integrada, identificando tanto sus fortalezas como sus lagunas y señalando las direcciones de reforma más urgentes. La Ley 24.240 de Defensa del Consumidor (1993) y sus modificaciones constituyen el núcleo del sistema tuitivo. Los artículos 8 bis, 9, 10 y siguientes establecen los principios generales de la relación de consumo, información, buena fe, trato digno y no discriminación, que son plenamente aplicables a la contratación electrónica. El artículo 40 y 40 bis CCCN establecen la responsabilidad objetiva y solidaria de los proveedores y la responsabilidad del Estado por omisión de control, respectivamente. Sin embargo, la ley fue concebida en un contexto tecnológico radicalmente distinto al actual, y muchas de sus disposiciones requieren una actualización que las adapte a las realidades del comercio electrónico, las plataformas de intermediación y los sistemas de inteligencia artificial. El Código Civil y Comercial de la Nación (Ley 26.994, 2015) representó un avance significativo al incorporar un capítulo específico sobre contratos de consumo (arts. 1092 a 1122) y contratos celebrados a distancia y por medios electrónicos (arts. 1105 a 1117). Estos artículos establecen un sistema coherente de protección que incluye los requisitos de información previa (art. 1107), la forma de la aceptación (art. 1108), el lugar de celebración del contrato (art. 1109) y el derecho de arrepentimiento (art. 1110). Los artículos 1092 y 1093 definen el contrato de consumo y las relaciones de consumo, mientras que los artículos 1094 y 1095 establecen los principios de interpretación favorables al consumidor. Esta sistematización normativa proporciona una base sólida para la protección del consumidor electrónico, aunque no aborda específicamente la hipervulnerabilidad digital ni contempla los desafíos de los sistemas de IA. La Ley 25.326 de Protección de los Datos Personales y su decreto reglamentario establecen el marco para el tratamiento de datos en Argentina, aunque con limitaciones evidentes frente a las realidades del *big data* y la inteligencia artificial. La Resolución 139/2020 del SIGEN ha actualizado algunos aspectos de la seguridad en el tratamiento de datos en el sector público, pero el sistema argentino requiere una reforma profunda para estar a la altura de los estándares internacionales. Las principales deficiencias identificadas por la doctrina incluyen: la ausencia de un concepto de datos sensibles suficientemente amplio para abarcar los datos biométricos y de comportamiento generados por los sistemas de IA; la inexistencia de un régimen específico de portabilidad de datos; la falta de un derecho a la explicación

de decisiones automatizadas; y la insuficiencia de los recursos y atribuciones de la Agencia de Acceso a la Información Pública como autoridad de aplicación. En el plano del derecho internacional de los derechos humanos, Argentina ha ratificado la Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores (CIDHPM, 2015), instrumento que establece el derecho de las personas mayores a la protección en sus relaciones con el sector privado y el mercado. Este instrumento, de aplicación directa en el ordenamiento jurídico argentino con jerarquía supralegal, proporciona un fundamento de derechos humanos para la protección reforzada de los adultos mayores como consumidores electrónicos hipervulnerables. Su artículo 30 reconoce específicamente el derecho de las personas mayores a acceder a los servicios de la sociedad de la información, incluyendo internet, lo que implica no solo el acceso formal sino el acceso en condiciones de seguridad y con las garantías necesarias para el ejercicio pleno de su autonomía. Desde una perspectiva de prospectiva normativa, la protección del consumidor electrónico hipervulnerable en Argentina requiere avanzar en al menos tres direcciones. La primera es la sanción de una ley de protección de datos personales modernizada, que incorpore los estándares del RGPD y establezca un régimen específico de protección para los datos de consumidores hipervulnerables. La segunda es el desarrollo de un marco regulatorio para la inteligencia artificial que prohíba los sistemas de alto riesgo en las relaciones de consumo que afectan a colectivos vulnerables y establezca requisitos de transparencia, auditoría y rendición de cuentas para todos los sistemas de IA utilizados en el mercado digital. La tercera es la creación de una agencia especializada en protección del consumidor digital, con recursos técnicos y legales suficientes para supervisar las prácticas de las grandes plataformas, investigar las denuncias de consumidores hipervulnerables y aplicar sanciones disuasorias a los proveedores que incumplen sus obligaciones. La articulación de todos estos elementos normativos con los principios del derecho comparado europeo (AI Act, DSA, RGPD) y con la jurisprudencia argentina en desarrollo constituye el marco de referencia desde el cual debe construirse una respuesta jurídica adecuada a los desafíos del consumidor electrónico hipervulnerable en la Argentina del siglo XXI. El análisis del marco normativo argentino permite identificar un patrón característico de los sistemas jurídicos en transición hacia la era digital: la existencia de principios y valores sólidos como el principio *pro consumatore*, la buena fe, la responsabilidad objetiva del proveedor y la

nulidad de las cláusulas abusivas, que proporcionan fundamento normativo suficiente para responder a los nuevos desafíos, pero cuya aplicación efectiva requiere un esfuerzo hermenéutico y una actualización conceptual que no siempre se producen con la velocidad que la tecnología demanda.

La brecha entre el derecho enunciado y el derecho aplicado es, en el campo del consumidor digital hipervulnerable, especialmente pronunciada. Cerrar esa brecha es una responsabilidad compartida del legislador, la jurisprudencia, la doctrina, las instituciones públicas de protección del consumidor y los operadores privados del derecho, entre los que la figura del notario ocupa un lugar de relevancia particular.

IV. Referencias bibliográficas

Barocelli, S. S., "Hacia la construcción de la categoría de consumidores hipervulnerables", *La Ley*, 2018-F, 929.

Cámara de Apelación de Morón. (2025). “PEA c/ BDLPDBA y otros s/ medida cautelar”, la Sala II de la Cámara Civil y Comercial de Morón, *Causa MO-30821-2025*. Resolución judicial sobre phishing y consumidor hipervulnerable. Poder Judicial de la Provincia de Buenos Aires. https://www.diariojudicial.com/news-102261-hipervulnerable-hiperprotegido

Chamatrópulos, D., *Estatuto del Consumidor Comentado*, La Ley, 2019.

CIDH, Opinión Consultiva OC-29/24 de 11/11/2024 sobre *Contenidos en redes sociales y otros servicios de internet*.

Código Civil y Comercial de la Nación. (2015). *Ley 26.994*. Honorable Congreso de la Nación Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-26994-235975

Colina, C. (2023) Manipulación algorítmica y sesgo psicosocial en redes sociales, 10.62876/tc.vi46.6219. https://www.researchgate.net/publication/385333016_Manipulacion_algoritmica_y_sesgo_psicosocial_en_redes_sociales/citation/download

Colombo, M. (2023). La manipulación algorítmica: una problemática de la revolución 4.0 que colisiona con el derecho a la libertad de expresión y el derecho a la información. Sup. Innovación y Derecho 2023 (agosto), 1. LA LEY 2023-D. Cita: TR LALEYAR/DOC/1806/2023.

Consejo de Europa, *Convención Marco sobre IA, DDHH, Democracia y Estado de Derecho* (Vilnius, 2024).

Consejo de Notariados de la Unión Europea (CNUE). (2025). *AI Handbook for Notaries*. CNUE.

Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores (CIDHPM). (2015). *Organización de los Estados Americanos (OEA)*.

https://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_A-70_derechos_humanos_personas_mayores.pdf
Convención sobre los Derechos de las Personas con Discapacidad. (2006). *Naciones Unidas*. https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html
Corvalán, J. G. (2018). Inteligencia artificial: Retos, desafíos y oportunidades. *Rivista di Diritto, Media e Tecnologia*, 1(1), 1–27. https://www.redalyc.org/journal/5340/534057837015/html/
CSJN, "Halabi, Ernesto c/ PEN", 24/02/2009, *Fallos* 332:111.

CSJN, "Padec c/ Swiss Medical S.A.", 21/08/2013, *Fallos* 336:1236.

Fineman, M. (2008). The vulnerable subject: Anchoring equality in the human condition. *Yale Journal of Law & Feminism*, 20(1), 1–23. https://openyls.law.yale.edu/server/api/core/bitstreams/f23fa6fb-d926-43dd-8627-d880c7337a8a/content
Gil Domínguez, A., *La regla de reconocimiento constitucional argentina*, Ediar, 2007. | Constitucionalización derecho privado.

Harari, Y. N. (2016). *Homo Deus: A brief history of tomorrow*. Harper.
Hernández, C. A. - Frustagli, S., "La hipervulnerabilidad del consumidor", *Revista de Derecho Comercial y de las Obligaciones*, 2017-B.

https://aldiaargentina.microjuris.com/2026/02/10/doctrina-incidencia-de-las-nuevas-tecnologias-en-la-voluntad-juridica-aproximacion/
Kemelmajer de Carlucci, A., "Las personas vulnerables en el derecho privado", *Revista de Derecho Privado y Comunitario*, 2018-3.

Lastra, A. (2016). El poder del prosumidor. Identificación de sus necesidades y repercusión en la producción audiovisual transmuda. Revista ICONO14 – Revista Científica De Comunicación Y Tecnologías Emergentes, 14(1), 71-94. https://doi.org/10.7195/ri14.v14i1.902
Ley 24.240. (1993). *Ley de Defensa del Consumidor*. Honorable Congreso de la Nación Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-24240-639
Ley 25.326. (2000). *Ley de Protección de los Datos Personales*. Honorable Congreso de la Nación Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-25326-59508

Ley 26.061. (2005). *Ley de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes*. Honorable Congreso de la Nación Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-26061-110778

Llaneza, P. (2019) “Dataismo”y “ en Datanomics. Deusto.

Llano Fernandez (2020) El mercado de los datos personales: la influencia del bigdata en el remarketing. Tesis de grado Facultad de Ciencias económicas yempresariales Universidad de León. Disponible en: https://buleria.unileon.es/bitstream/handle/10612/12381/LlanoFernandezAna.pdf?sequence=1

Lorenzetti, R. L., *Consumidores*, 2.ª ed., Rubinzal-Culzoni, 2009.

Negri, N. (2025) *Contratación electrónica: un análisis en el contexto de la sociedad digital* en Anales de la Universidad Notarial Argentina | N° 2 abril 2025 | Electrónica ISSN 3072-6948.

Palacios, A., *El modelo social de discapacidad*, CINCA, 2008.

Picasso, S., "Las responsabilidades en la contratación electrónica", *Revista de Derecho Comercial*, 2022-A.

Pizarro, R. - Vallespinos, C., *Instituciones de Derecho Privado. Obligaciones*, Hammurabi, t. 6, 2022.

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales o DSA). *Diario Oficial de la Unión Europea*, L 277, 1–102. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022R2065

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

Resolución 139/2020. (2020). *Sindicatura General de la Nación (SIGEN)*. Ministerio de Economía de la República Argentina.

Rubio García, R. (2014): “Twitter y la teoría de la Agenda Setting: mensajes dela opinión pública digital”. Estudios sobre el Mensaje Periodístico. Vol. 20, Núm.1 (enero-junio), págs.: 249264. Madrid, Servicio de Publicaciones de la Universidad Complutense.

Sadin, E. (2018) “De la revolución digital al advenimiento de una antro-biología” en La humanidad aumentada. Caja negra editora.

Salierno, K. V. y Spina, M. V. (2026). *Guía de Actuación Notarial en entornos digitales y comparecencia remota de personas en situación de vulnerabilidad. El notario como garante de los derechos digitales.* Ed. Dilalla.

Salierno, K., V (2024). *Derechos digitales de la infancia*. Ed. Astrea.

Schab, E. (2018), “Minería de datos y visualización de información” en Red UNCI-UNNE XX Whorkshop de investigaciones en Ciencias de la Computación, ISBN978-987-3619-27-4 Disponible en: https://ria.utn.edu.ar/xmlui/bitstream/handle/20.500.12272/3567/Miner%C3%ADa%20de%20Datos%20y%20Visualizaci%C3%B3n%20de%20Informaci%C3%B3n.pdf?sequence=1

Shina**.** F. **(**2026) El ocaso de la teoría general del acto jurídico. Id SAIJ: DACF260011. https://www.saij.gob.ar/fernando-shina-ocaso-teoria-general-acto-juridico-dacf260011-2026-02-12/123456789-0abc-defg1100-62fcanirtcod?q=fecha-rango%3A%5B20250901%20TO%2020260301%5D&o=7&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=69

Sozzo, G., *El consumidor en el nuevo Código Civil y Comercial*, Rubinzal-Culzoni, 2016. | Perspectiva crítica.

Stiglitz, G. A., *Defensa del consumidor*, Rubinzal-Culzoni, 2020.

Sunstein, C. R. (2013). *Simpler: The future of government*. Simon & Schuster.
Sunstein, C. R. y Thaler, R. H. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.
Tambussi, C. E., *El consumo como derecho humano*, Universidad, 2014. | Integración DDHH-consumo.

Tapia Rodríguez, Mauricio. «Autonomía de la voluntad y derechos fundamentales en la era digital» Revista de Derecho Privado, Universidad de Chile, 2021.
UNESCO, *Recomendación sobre la ética de la inteligencia artificial*, 2021, párrs. 88-104.

Vera Santos, J (2025) *Libertad de Información Veraz y manipulación algorítmica.* Revista de las Cortes Generales. ISSN: 0213-0130. ISSNe: 2659-9678N.º 120, Segundo semestre (2025): pp. 85-129 https://doi.org/10.33426/rcg/2025/120/1878
Vidal, C (2026). Incidencia de las nuevas tecnologías en la voluntad jurídica. Aproximación. Doctrina**.** MJ-DOC-18613-AR||MJD18613
Wajntraub, J., *Régimen jurídico del consumidor*, Rubinzal-Culzoni, 2017.

Wierzba, Sandra M. Responsabilidad civil y automatización: hacia nuevos paradigmas. Publicado en: LA LEY 02/08/2023, 1. Cita: TRLALEY AR/DOC/1602/2023
Yeung, K., "'Hypernudge': Big Data as a Mode of Regulation by Design", *Information, Communication & Society*, 20(1), 2017, pp. 118-136.

Zuboff, S., *The Age of Surveillance Capitalism*, PublicAffairs, 2019.