

ÍNDICE GENERAL

PALABRAS PREVIAS	9
ABREVIATURAS	21

CAPÍTULO I

VULNERABILIDAD DIGITAL Y CONSTITUCIONALISMO

WALTER F. CARNOTA - LUCAS DE VENEZIA

§ 1. Introito	25
a) Su actualidad	26
b) Un nuevo «momento constitucional»	27
§ 2. El ámbito de la normativa regulatoria: nacional e internacional	27
§ 3. Los retos a la intimidad o privacidad	28
§ 4. La libertad de expresión en la era digital	30
§ 5. La igualdad en la era digital	32
§ 6. Derecho a la educación y acceso a la información virtual	33
§ 7. La gobernanza de Internet y la soberanía digital	34
§ 8. El futuro del trabajo y los derechos laborales en la era digital	36
§ 9. Los derechos de índole procesal: el acceso a la justicia	38
§ 10. Conclusiones	38

CAPÍTULO II

VULNERABILIDAD DIGITAL Y SU MARCO CONCEPTUAL

ÚRSULA BASSET

§ 1. Vulnerabilidad, un tropo ineludible del derecho de hoy	41
---	----

§ 2. La evolución del concepto de vulnerabilidad: de la vulnerabilidad categorial (fija) a una vulnerabilidad democratizada y universal (ubicua)	42
a) La vulnerabilidad categorial	43
b) Vulnerabilidad universal	44
§ 3. Aproximación semántica al término	45
§ 4. Pragmática de la palabra «vulnerabilidad» en los documentos internacionales	46
a) En el ámbito de los documentos internacionales	47
b) Instrumentos regionales adoptados por la OEA	50
§ 5. Conceptualizando la vulnerabilidad	65
a) Las ventajas de los contornos difusos de la definición	66
b) Funciones de la perspectiva de vulnerabilidad	66
c) Proyección biográfica de la perspectiva de vulnerabilidad: la prevención del daño y el fortalecimiento temprano de redes	67
§ 6. Criterios para una aplicación proporcionada y prudente de la perspectiva de vulnerabilidad	68
a) Aplicación de la perspectiva de vulnerabilidad en tres funciones	69
b) Criterios de aplicación en la función rectificadora de la norma	69
c) Diferencia entre la función rectificadora de la ley y la ley injusta o inconstitucional	70
§ 7. Vulnerabilidad y dignidad humana: una herramienta de revisión del derecho privado decimonónico y su paradigma del fuerte	72
§ 8. La vulnerabilidad digital	74

CAPÍTULO III

VULNERABILIDAD DIGITAL Y EDUCACIÓN

KARINA VANESA SALIERNO

§ 1. Introducción	77
§ 2. La brecha digital profundiza la desigualdad educativa	82
§ 3. Vulnerabilidad digital estructural	85
§ 4. La falta de habilidades básicas digitales	93
§ 5. «Reskilling needs», adaptación e interdisciplina	95
§ 6. ¿Tecnología vs. humanidad?	100
§ 7. El dilema de «Chat GPT», solo el comienzo	102
§ 8. Aplicaciones de IA al proceso educativo: no juegues, programa el juego	105
§ 9. ¿Cómo influye la IA en el método científico?	108
§ 10. Conclusiones y prospectiva	110

CAPÍTULO IV

VULNERABILIDAD DIGITAL ADMINISTRATIVA

MARÍA JOSÉ RODRÍGUEZ

§ 1. Introducción	111
-------------------------	-----

§ 2.	La vulnerabilidad como consecuencia de la brecha digital o dificultades en el uso de la tecnología	114
a)	La transferencia de cargas a los particulares administrados y usuarios y el agobio de estos	117
b)	La obstrucción del acceso a trámites administrativos o servicios públicos por las dificultades tecnológicas viola los principios tradicionales del servicio público y refuerza posibles vulnerabilidades	118
§ 3.	El empleo de la tecnología y el desafío de no caer en la razón instrumental. La degradación del ser humano que apareja esta última, así como de sus derechos	119
§ 4.	La desconfiguración del derecho administrativo por la globalización y la tecnociencia (prevalencia de la razón instrumental)	122
—	Globalización, tecnociencia y el déficit democrático que aparejan. Su incidencia en los derechos fundamentales	125
§ 5.	Los derechos y principios digitales de la UE: ¿al rescate de un personalismo solidario? Su fuerza expansiva	126
§ 6.	Prognosis conclusiva	127

CAPÍTULO V

VULNERABILIDAD DIGITAL Y GOBERNANZA

MARIANA SÁNCHEZ CAPARRÓS

§ 1.	Irrupción de la IA generativa	129
§ 2.	IA generativa en el ámbito judicial	132
a)	Introducción	132
b)	La importancia de la letra pequeña de los términos de privacidad	134
—	La política de privacidad para los servicios de OpenAI: consideraciones relevantes	135
I.	Política de privacidad de OpenAI para ChatGPT y GPT-4	135
I.1	Información personal que OpenAI recolecta	135
I.2	Cómo utiliza la información personal OpenAI	136
I.3	Divulgación de información personal	137
I.4	Retención de información personal	138
I.5	Almacenamiento y procesamiento de información	138
II.	Política de privacidad de OpenAI para usuarios de empresa (ChatGPT-Team, ChatGPT Enterprise y plataforma API)	138
II.1	Posee y controla sus datos	139
II.2	Decide quién tiene acceso a sus datos	139
II.3	Preguntas frecuentes	139
c)	Conclusiones: las políticas de privacidad como un elemento relevante a considerar	141
§ 3.	Tensiones entre la publicidad procesal y la protección de datos en la era de la IA generativa	141
a)	Introducción: la gestión judicial desde la dimensión digital	141

b) La publicidad procesal y la protección de datos personales en la era digital	143
1. La publicidad procesal	143
2. El derecho a la protección de los datos personales	144
c) Conclusiones: límites para el uso de IA generativa en el sector público	146
§ 4. Cierre	148

CAPÍTULO VI

**VULNERABILIDAD DIGITAL
Y CIBERDELITOS**

MARCO ROSSI

§ 1. Introducción	151
§ 2. Definición de conceptos	152
§ 3. Percepción de seguridad en línea: la buena fe digital en redes sociales	154
a) ¿Cómo ocurrían las comunicaciones interpersonales no presenciales antes de Internet?	154
b) ¿De qué manera se generaban consecuencias jurídicas con ese tipo de interacciones?	155
c) Los comportamientos considerados seguros en la era del papel (sellos, firmas, marcas de agua, etcétera) y el concepto de buena fe en esos negocios jurídicos	157
d) ¿Cómo ocurren las interacciones personales no presenciales en la actualidad?	158
e) ¿Qué cambios implica en materia de seguridad jurídica? ¿Cómo sé con quién interactúo? ¿Cómo llevar las consecuencias del mundo digital al analógico?	159
1. Cambios en materia de seguridad jurídica	159
2. ¿Cómo sé con quién interactúo?	159
f) Llevar las consecuencias del mundo digital al analógico	160
§ 4. Interacciones personales e interacciones anónimas	160
a) ¿Qué implica la presencia personal para la realización de negocios jurídicos? ¿De qué modo se realizan las interacciones interpersonales con consecuencias jurídicas de forma asincrónica y no presencial sin tecnología digital?	160
b) ¿Por qué es posible separar la identidad personal de la identidad digital en Internet? ¿Qué es la huella digital? ¿Por qué hay personas que prefieren ser anónimas en línea?	162
§ 5. El ejercicio de la libertad de opinión mediante tecnologías de la Web 2.0	162
a) ¿Qué es la libertad de opinión o libertad de prensa? ¿Qué relación tiene con la constitución, el Estado de derecho y la democracia?	162
b) ¿Por qué las redes sociales son el «ágora» de la antigua Grecia del día de hoy?	164
c) ¿Por qué las mismas garantías de libertad de opinión deben estar salvaguardadas en las interacciones en redes sociales?	165
§ 6. La figura del influencer y el poder de las comunidades	166
a) ¿De qué manera se generan comunidades digitales con poder de generar cambios en el mundo real?	166
b) ¿Cómo generan comunidades los influencers? Liderazgo de comunidades mediante la generación de vínculos de afinidad por generación de contenidos	168

c) ¿Cuál es la responsabilidad de los influencers por las acciones de los miembros de su comunidad? ¿Cuál es la responsabilidad del influencer por aquello que publica en sus plataformas?	169
§ 7. La cultura de la cancelación y la justicia por mano propia	170
a) Imagen negativa vs. imagen positiva	171
b) ¿Por qué las «fake news» se viralizan? ¿De qué manera se puede ejercer el derecho a réplica cuando no ocurrió en un medio tradicional?	172
c) ¿Qué implica cancelar a alguien? ¿Qué consecuencias éticas, jurídicas y económicas tienen las campañas de cancelación? ¿Por qué es equiparable a la justicia por mano propia?	173
§ 8. Intrusión no consentida en la vida personal: vulneración intencionada de información	175
a) ¿De qué manera la intrusión no consentida en la vida personal representa una violación de la privacidad y cuáles son sus principales métodos?	175
b) ¿Cómo afectan estas intrusiones a la percepción de seguridad personal en el entorno digital y cuál es el impacto en la vida cotidiana de las víctimas?	176
c) En el marco legal actual, ¿qué herramientas jurídicas están disponibles para las víctimas de estas intrusiones y cómo se pueden fortalecer estas medidas para ofrecer una mayor protección?	177
§ 9. Doxéo: hackeo y exposición de datos personales	179
a) ¿Qué técnicas son comúnmente empleadas en el proceso de «doxing» y cómo pueden los individuos protegerse de esta exposición no consentida?	179
b) Dado el aumento de casos de doxing, ¿cuál es el papel de las plataformas digitales y redes sociales en la prevención y mitigación de estos ataques?	180
c) ¿Cómo pueden las leyes adaptarse para abordar más eficazmente el doxing, considerando el equilibrio entre la libertad de expresión y la protección de la privacidad?	181
§ 10. El castigo digital y sus consecuencias en el mundo analógico	182
a) ¿De qué manera el castigo digital, como la cultura de la cancelación, trasciende al mundo analógico y afecta la vida profesional y personal de los individuos?	182
b) Frente al fenómeno del castigo digital, ¿cuál debería ser la respuesta de la sociedad y del sistema legal para proteger tanto la libertad de expresión como el derecho a no ser sometido a un castigo desproporcionado por la opinión pública?	184

CAPÍTULO VII

VULNERABILIDAD DIGITAL Y SALUD

MARÍA ISABEL IÑIGO PETRALANDA

§ 1. Introducción	187
§ 2. El contexto de la estrategia mundial de salud digital	189
§ 3. Estatuto moral de la persona del participante en la bioética personalista	193
§ 4. Pautas para la Investigación con seres humanos	194
a) Estándares y orientación operativa para la revisión ética de investigaciones relacionadas con la salud de participantes humanos	194

b) Pautas Éticas Internacionales en las Normas para la toma del Consentimiento Informado en el Consejo de Organizaciones Internacionales de las Ciencias Médicas (CIOMS)	195
c) Requisitos que hacen a una investigación «ética»	196
§ 5. Investigación biomédica y protección del participante	197
§ 6. Nuevas formas de investigación biomédica. Los Ensayos Clínicos Descentralizados (ECD) en el contexto de las nuevas tecnologías	199
§ 7. Consentimiento informado como proceso comunicativo	202
§ 8. Componentes del consentimiento informado	203
§ 9. Valoración del CEI sobre el consentimiento informado en investigación prestado por nuevas tecnologías	204
a) Consentimiento Informado Manuscrito Presencial (CIMP)	205
b) Consentimiento Informado Electrónico Presencial (CIEP)	205
c) Consentimiento Informado Electrónico Remoto (CIER)	205
d) Seis etapas de un consentimiento informado con nuevas tecnologías	206
§ 10. Marco regulatorio de elementos descentralizados en estudios de farmacología clínica en la Argentina	207
§ 11. Conclusiones	208

CAPÍTULO VIII

**VULNERABILIDAD DIGITAL
Y DERECHO DE DAÑOS**

FERNANDO ALFREDO UBIRÍA - EMILIANO CARLOS LAMANNA GUIÑAZÚ

§ 1. Prefacio	211
§ 2. Primer trazo evolutivo de la responsabilidad civil en la Argentina: de la deuda por el actuar negligente al crédito por responsabilidad legal. Los «factores» López Olaciregui e Ivonne Lambert-Faivre ingresan en el ecosistema del daño	213
§ 3. Segundo trazo evolutivo en la responsabilidad civil: el «factor» De Lorenzo y la noción del daño «injusto» y la relectura de la antijuridicidad en el ecosistema reparador	216
§ 4. De reformas legislativas fallidas al Código Civil y Comercial 2015	217
§ 5. Un párrafo aparte: la prevención del daño. «Quid» del «compliance» como modelo preventivo	218
§ 6. Paradigmas del responder	224
§ 7. Rol del daño jurídico en el sistema del responder civil	225
§ 8. Ecosistema de daños resarcibles y el numeral de posibles abordajes desde la perspectiva de la vulnerabilidad: daños en redes sociales; «fake news»; datos personales e Inteligencia Artificial	226
a) Daños en redes sociales. La sociedad de la información: ¿un ecosistema jurídico transversal?	227
b) «Fake news»	228
c) Datos personales. La Big Data y el Data Mining como la plataforma de compra y venta en la mercadotecnia 4.0	230
d) Inteligencia artificial	232

§ 9. Los dilemas éticos que plantea la Revolución Industrial 4.0: ¿Hacia una vulnerabilidad regulada?	235
---	-----

CAPÍTULO IX

**VULNERABILIDAD DIGITAL Y NIÑOS,
NIÑAS Y ADOLESCENTES**

ZARINA ROSS

§ 1. Introducción	237
§ 2. El derecho a la intimidad, su regulación y el marco normativo con relación a la infancia	238
a) El derecho a la intimidad y su regulación en el derecho argentino	239
b) Convención sobre los Derechos del Niño	239
c) Las 100 reglas de Brasilia sobre acceso a la justicia de las personas en condición de vulnerabilidad	240
d) Observación General n° 25 (2021) sobre los derechos del niño en relación con el entorno digital	241
e) Ley 26.061 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes	242
f) Ley 25.326 de Protección de Datos Personales	243
g) Ley 26.522 de Servicio de Comunicación Audiovisual	244
h) Ley 27.699, «Protocolo modificatorio del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal»	245
i) «Softlaw»	245
§ 3. La infancia en entornos digitales	247
a) Ciudadanía digital	247
b) El derecho a la intimidad y los peligros a los que se ven expuestos niños, niñas y adolescentes en el entorno digital	249
c) El «sharenting» la responsabilidad parental	253
§ 4. Conclusión	257

CAPÍTULO X

VULNERABILIDAD DIGITAL Y CRIPTOACTIVOS

SEBASTIÁN HEREDIA QUERRO - FRANCESCA PETRAZZINI

§ 1. Introducción: ¿Contratos cada vez más complejos, mejores contratos?	261
§ 2. Web3, Blockchain & Smart Contracts	266
§ 3. Primeras aproximaciones al «Legal Design»: ¿Qué es, cómo surge y para qué sirve?	270
§ 4. El papel del «Diseño Legal» de «Contratos» en la protección de los usuarios y consumidores	280
a) Casos prácticos de implementación	281
b) Regulación en la Argentina	286
§ 5. Aproximaciones a las «Dark Patterns». Regulaciones novedosas	288
a) «Legal Design» & «Dark Patterns»	289
b) Protección de menores: el caso de California	290

§ 6. El «Legal Design» de «Smart Contracts»	293
§ 7. Caso práctico de implementación del «Legal Design» en un proyecto de tecnología «blockchain»	298
§ 8. Conclusiones	303

CAPÍTULO XI

VULNERABILIDAD DIGITAL Y GÉNERO

MACARENA BARICCO PRATS

§ 1. Introducción	307
§ 2. La imagen y su manipulación	308
§ 3. ¿De qué hablamos cuando hablamos de «DeepFakes»?	310
§ 4. ¿Para qué se utilizan los «DeepFakes»?	312
§ 5. El peligro «fake porn»	313
§ 6. El «fake porn» como violencia digital	316
§ 7. Normativa sobre «fake porn»	317
§ 8. El rol de las redes sociales y las medidas a adoptar	320
§ 9. Conclusión	322

CAPÍTULO XII

VULNERABILIDAD DIGITAL Y CONSUMO

JOSÉ H. SAHIÁN

§ 1. Protección general del consumidor en los entornos digitales	323
a) Introducción metodológica	323
b) La sociedad de consumo digital: sus relaciones y los nuevos paradigmas	324
c) Relación de consumo digital	325
d) Legislación general de los consumidores digitales	327
e) Derechos fundamentales de los consumidores digitales	330
f) El derecho a la información digital	337
g) Principios de defensa de los consumidores digitales	340
h) Solución de conflictos digitales: ODR	341
§ 2. Hipervulnerabilidad «in genere»	342
§ 3. Hipervulnerabilidad digital: dimensiones normológicas objetivas	346
a) Nociones generales	346
b) Unión Europea	347
c) Derecho internacional	348
d) Derecho supranacional	350
§ 4. Hipervulnerables digitales: subjetividades especiales	351
a) Etaria: niños, niñas y adolescentes	351
b) Consumidores con discapacidad	354
c) Vulnerabilidad sanitaria	354
d) Vulnerabilidad financiera	355

e) Debilidad volitiva	356
f) Desafío de IA. Discriminación	357
g) Discriminación: precios personalizados	358
h) Tutela efectiva de los consumidores digitales	361
§ 5. Conclusiones	362

CAPÍTULO XIII

**VULNERABILIDAD DIGITAL
EN LA TERCERA EDAD**

MARCELO BRASBURG - MARÍA ANDREA ROMERO

§ 1. Tecnología y adultos mayores en la Argentina: un estudio cuantitativo y cualitativo	365
a) Metodología de investigación	365
b) Factores socio-económicos y demográficos	366
c) Nivel educativo	367
d) Rangos etarios	369
e) Cuestión de género	370
f) Migración al mundo digital	371
§ 2. El camino de inclusión: adaptación y educación	373
a) ¿Vuelta al papel o educación?	373
b) Período de transición	374
c) Hacia la telefonía celular en el uso de Internet	377
§ 3. TIC para adultos mayores y su regulación	379
a) Derecho a la educación digital	380
b) Accesibilidad en oficinas públicas y servicios sociales	382
c) Reglamentación legal	383
§ 4. Acceso a la justicia digital	384
a) Transformación digital de la justicia	384
b) Causales impeditivas de acceso a la justicia para adultos mayores	386
1. Vulnerabilidad en los adultos mayores	386
2. Brecha digital	387
3. Maltrato	387
4. Lenguaje complejo	388
c) Medidas procesales	389
BIBLIOGRAFÍA GENERAL	391