

ÍNDICE GENERAL

PRESENTACIÓN DE LA COLECCIÓN	7
ABREVIATURAS	17

A. DERECHO INFORMÁTICO APLICADO

1. ACTUALIDAD EN MATERIA DE TRIBUTACIÓN DE LA ECONOMÍA DIGITAL

ISMAEL LOFEUDO

§ 1. Introducción	23
§ 2. La Economía digital desde la perspectiva de la OCDE	26
§ 3. El Impuesto sobre los Ingresos Brutos. Modificaciones recientes a los códigos fiscales provinciales	31
a) Los cambios en la provincia de Buenos Aires	32
b) La situación en el resto de las jurisdicciones	36
1. La provincia de Tucumán	38
2. La provincia de Mendoza	39
3. La provincia de La Pampa	39
4. La provincia de Salta	39
5. La provincia del Chaco	39
6. La provincia de Neuquén	40
7. La provincia de San Juan	40
8. La provincia de San Luis	40
§ 4. Los agentes de recaudación en la Argentina	41
§ 5. El nuevo régimen de retención sobre billeteras virtuales en la Provincia de Buenos Aires	42
§ 6. Conclusión	44

2.**EL TELETRABAJO INTERNACIONAL**

Análisis de algunas cuestiones que se plantean
en el Derecho Internacional Privado

CORINA ANDREA IUALE

§ 1. El teletrabajo	47
a) La diligencia del teletrabajador	49
b) La protección de datos	49
c) El acuerdo de teletrabajo	50
§ 2. El teletrabajo internacional	50
a) Las calificaciones	51
b) Ley aplicable al teletrabajo internacional	52
c) El teletrabajo y el cumplimiento normativo	53

3.**LA IMPUTACIÓN JURÍDICA DE LA FIRMA DIGITAL**

ANÍBAL PARDINI

§ 1. Planteo del problema	55
§ 2. La tecnología como factor de riesgo jurídico	56
§ 3. La firma digital	58
a) Actores del sistema	58
b) Su abordaje	61
c) Evolución normativa	63
d) El escenario actual	64
— La Plataforma de Firma Digital Remota (PFDR)	64
I. Escenario 1	67
II. Escenario 2	69

4.**DE LA IDENTIFICACIÓN HUMANA
A LA PROTECCIÓN DE DATOS GENÉTICOS**

MARÍA PAULINA CASARES SUBÍA

§ 1. Introducción	73
§ 2. Identificación humana	74
§ 3. Bioinformática	76
§ 4. ADN	77
§ 5. Biobancos	78
§ 6. La protección de datos en la garantía de los derechos fundamentales	79
§ 7. Protección de datos	80
a) Historia y evolución de la protección de datos	81
b) Dato e información	81

§ 8. Situaciones legales	89
a) Diagnóstico Genético Preimplantacional (DGP)	89
b) Criopreservación de embriones	90
c) Fecundación de un óvulo con espermatozoides de dos varones	90
d) Donadores anónimos y problemas de filiación	91
e) Muestras médicas y laboratorios	91
f) En los centros de belleza	91
g) «Biohacking», transhumanismo, posthumano	92
§ 9. Conclusiones	93

5.

**LOS CONFLICTOS EN EL COMERCIO INTERNACIONAL,
LA RESOLUCIÓN DE DISPUTAS Y LA APARICIÓN
EN ESCENA DE UNA JUSTICIA PRIVATIZADA**

Las plataformas de Resolución de Disputas en Línea (ODR)

HANNAH FRANK - CARLOS DIONISIO AGUIRRE

§ 1. Introducción	95
§ 2. El arbitraje comercial internacional «on line»	96
a) Generalidades	96
b) Marco regulatorio	98
c) Respeto a su contemporaneidad y en miras al futuro	100
d) Principios rectores del arbitraje comercial internacional en línea	101
1. Transparencia	102
2. Independencia	102
3. Especialización	102
4. Consentimiento	102
5. Otros principios	102
e) Procedimiento del arbitraje comercial internacional «on line» o en línea	103
§ 3. Conclusiones	105

6.

**«SMART CONTRACTS»: CONCEPTO
Y APLICACIÓN LEGAL**

FERNANDO O. BRANCIFORTE

§ 1. Introducción	107
§ 2. Un poco de historia	108
§ 3. El ecosistema «blockchain»	109
§ 4. ¿Qué es un «smart contract»?	111
a) Características de los «smart contracts»	113
b) ¿El «smart contract» es realmente un contrato?	114
c) Su aplicación legal	118
d) Diferencia con los contratos electrónicos	119

e) Posibles conflictos respecto a su implementación	119
f) El rol del abogado frente al «smart contract»	124
§ 5. Conclusión	125

7.

PROTECCIÓN JURÍDICA DE DATOS DE CARÁCTER PERSONAL

ALEJANDRO KOHEN

§ 1. Génesis y desarrollo	127
§ 2. El derecho a la privacidad y protección de los datos personales	130
§ 3. Sistema de «data protection»	133
a) Principios relativos a las garantías mínimas que deberían preverse en la legislación nacional	134
b) Principios a la calidad de los datos	136
c) Principios relativos a la legitimación del tratamiento de datos	136
§ 4. Proyecto de reforma general de las Normas de Protección de Datos de la Unión Europea de 1995	137
§ 5. Hábeas data	138
a) Concepto	138
b) Naturaleza	139
c) Objeto y finalidades	140
d) Clases	141
1. Hábeas data informativo	141
2. Hábeas data aditivo	141
3. Hábeas data rectificador	142
4. Hábeas data preservador	142
5. Hábeas data cancelatorio o exclutorio	142
6. Hábeas data reparador	143
7. Hábeas data impugnativo	143
8. Hábeas data bloqueador	143
9. Hábeas data disociador	143
10. Hábeas data asegurador	143
e) Excepciones	143
f) Legitimación	144
g) Conclusión	144

8.

«RANSOMWARE AS A SERVICES». EL CRIMEN PERFECTO DESDE EL DISEÑO. PERSPECTIVA ANALÍTICA TÉCNICO JURÍDICA DESDE LA «GENERAL DATA PROTECTION REGLEMENT» (UE)

ALBERTO HERNÁN SAUL

§ 1. Criterios de análisis. Cuestiones preliminares. Perspectivas de futuro	145
---	-----

§ 2. Antecedentes	147
a) Marco conceptual técnico jurídico	147
b) Orígenes. Características esenciales, estructurales y funcionales	148
c) Cambio de paradigma. El futuro del «ransomware» a partir del año 2019	151
§ 3. «General Data Protection Reglament» (GDPR)	152
a) Marco teórico. Directrices y foco de análisis	152
b) GDPR, art. 4.12, “Brechas de seguridad”	153
c) GDPR, art. 5.f, 5.2, “Responsabilidad proactiva «accountability»”	154
d) GDPR, art. 32, “Seguridad de los datos personales”	155
— Seguridad del tratamiento	155
§ 4. Conclusión	157

9.

EL GOBIERNO ABIERTO COMO HERRAMIENTA DE EMPODERAMIENTO DE LAS PERSONAS

MARÍA VICTORIA SUKENIK

§ 1. Introducción	159
§ 2. Condiciones necesarias para que el Gobierno Abierto funcione	161
§ 3. La participación de mujeres y niñas en el Gobierno Abierto	163
§ 4. ¿Cómo el Gobierno Abierto podría contribuir a reducir la Brecha Digital de Género?	165
§ 5. Conclusiones	168

10.

EL DAÑO TECNOLÓGICO

Su conceptualización y necesidad de adaptación legal ante los problemas para establecer la responsabilidad civil en el contexto de las nuevas tecnologías

VÍCTOR MANUEL SALGADO MONTERROSA

§ 1. Prolegómenos sobre el concepto de Daño Tecnológico	171
§ 2. Nociones sobre la evolución del Derecho de Daños y su adaptación	173
§ 3. Algunas dificultades sobre la Responsabilidad Civil en el ambiente digital	175
§ 4. Delimitación conceptual del Daño Tecnológico	179
§ 5. Conclusión	183

11.

SEGURO DE RIESGOS CIBERNÉTICOS, LA PÓLIZA OBLIGATORIA

HUGO FABIÁN PÉREZ CARRETTA

§ 1. Introducción	185
§ 2. Concepto y caracteres distintivos del Riesgo Cibernético	186

§ 3. Riesgo cibernético asegurable	188
a) ¿Cómo se ve afectada una empresa si recibe un ciberataque?	189
b) ¿Cómo se protege una empresa al adquirir un seguro de riesgos cibernéticos? ..	189
c) El consentimiento de las partes, las actividades comprendidas y la suma asegurada	190
d) Conexión entre seguros cibernéticos y protección de datos personales	193
§ 4. Conclusiones	196

B. DELITOS INFORMÁTICOS

1.

POLÍTICA CRIMINAL Y DELITOS INFORMÁTICOS EN ARGENTINA

JOSÉ F. ARCE

§ 1. Introducción	201
§ 2. Política criminal y delitos informáticos	202
§ 3. Cibercrimen en el mundo	203
§ 4. ¿Qué pasó en Argentina? Surgimiento de la ley de delitos informáticos	204
a) ¿Qué dice esta ley?	205
b) ¿Quién la propuso y quiénes la discutieron?	205
c) ¿Cómo se acompaña desde el derecho procesal?	206
d) ¿Cómo acompaña estas reformas el Código Procesal Penal de la Nación?	208
e) ¿Y el agente encubierto?	208
§ 5. Delitos informáticos como política criminal en Argentina	209
a) ¿Cuáles son los modelos de intervención actuales?	209
1. Modelo concentrado	210
I. Ciudad Autónoma de Buenos Aires	210
II. ¿Quién se encarga de la investigación y de realizar la parte técnica de In-	
formática forense?	210
2. Modelo desconcentrado	211
I. Córdoba	211
II. ¿Quién se encarga de la investigación y de realizar la parte técnica de In-	
formática forense?	212
3. Modelo mixto	212
I. Ministerio Público Fiscal de la Nación	212
II. ¿Quién se encarga de la investigación y de realizar la parte técnica de In-	
formática forense?	212
4. ¿Y el resto del país, qué forma de intervención adopta?	213
b) ¿Qué modelo da mejor resultado?	213
c) ¿Cuál es la relación informática forense con el cibercrimen?	214
d) ¿Puede no haber mirada de género en las políticas criminales?	214
e) ¿Quiénes toman y/o controlan las decisiones en los casos concretos?	215
f) ¿Cuál es el rol de las fuerzas de seguridad?	216
g) ¿Qué rol tienen las fuerzas de la ley internacionales?	217

h) ¿Cuáles son los objetivos de los programas nacionales y organizaciones que trabajan la temática?	217
i) ¿Retener datos o no?	218
j) ¿Existen redes de cooperaciones nacionales o internacionales?	219
k) ¿Adhesión al Convenio de Budapest?	220
l) Nuestro país sigue una política criminal difusa en materia de cibercriminalidad	221
m) Ideas que suman al debate	222
§ 6. Palabras finales	223

C. LA PRUEBA DIGITAL

1.

**LOS NUEVOS VIEJOS RIESGOS DEL NEGOCIO:
GOBIERNO DE TI Y CIBERSEGURIDAD
FRENTE A LA INNOVACIÓN
Y LA TRANSFORMACIÓN DIGITAL**

FABIÁN DESCALZO

.....	227
-------	-----

2.

**LAS VÍAS PROCESALES PARA PROTEGER
LA DIGNIDAD DIGITAL**

BÁRBARA VIRGINIA PEÑALOZA

§ 1. Introducción	263
§ 2. Dignidad Digital	265
§ 3. Ataques digitales a la dignidad	267
a) Escraches	267
b) Amenazas, extorsión (sextorsión) y chantaje	270
c) Difusión no consentida de imágenes	271
d) Acoso digital o «ciberbullying»	273
§ 4. Elección de la vía procesal más adecuada	275
a) Legitimación sustancial pasiva y activa	275
b) Caminos procesales posibles	280
1. Justicia penal	281
2. Justicia civil	281
I. Acción de amparo	282
II. Acción de hábeas data	283
III. Medida autosatisfactiva	284
IV. Acción preventiva de daños	286
V. Acción resarcitoria por daños y perjuicios	291
§ 5. Conclusiones	291

D. ANÁLISIS JURISPRUDENCIAL**1.****DE LA INTERPRETACIÓN COHERENTE Y ARMÓNICA
DE LAS NORMAS. EL CASO «ANTENAS» A LA LUZ
DEL VOTO MAYORITARIO DE LA CORTE SUPREMA DE JUSTICIA**

JOSÉ ARÁOZ FLEMING

§ 1. Análisis del caso	297
§ 2. Conclusión	308
BIBLIOGRAFÍA GENERAL	309