



ÍNDICE GENERAL

AGRADECIMIENTOS	9
PRÓLOGO	21
ABREVIATURAS	25
INTRODUCCIÓN	31
CAPÍTULO I	
LA SOCIEDAD DE LA INFORMACIÓN EN LA ERA DE LA REVOLUCIÓN DIGITAL	
DE LA SOCIEDAD ANALÓGICA DEL SIGLO XX A LA SOCIEDAD DIGITAL DE LA CUARTA REVOLUCIÓN INDUSTRIAL DEL SIGLO XXI	
§ 1. La sociedad de la información en la era digital	55
§ 2. Toma de posición y valoración provisoria	72
CAPÍTULO II	
LA REFORMULACIÓN DEL DERECHO A LA PRIVACIDAD	
LA POSPRIVACIDAD, LA AUTODETERMINACIÓN INFORMATIVA Y EL DERECHO AL ANONIMATO	
§ 3. El principio de reserva o derecho a la privacidad	75
§ 4. La privacidad en el siglo XXL la era de la posprivacidad	79
§ 5. El teléfono celular inteligente («smartphone») o terminal móvil multiplataforma de convergencia de TIC como extensión de la privacidad	83
a) Caso «Riley v. California» (2014)	89
b) Caso «G.F.J. Nulidad» (CNCC, 31 de julio de 2018)	91
§ 6. La posprivacidad, la interpretación dinámica de la autodeterminación informativa y el derecho al anonimato	93
a) La posprivacidad	93
b) El derecho a la autodeterminación informativa	94
1. Caso «Trabajo Rueda v. España» (TEDH, 2017)	96
2. Caso «Benedik v. Slovenia» (TEDH, 2018)	97
3. Caso «Carpenter v. United States» (2018)	98
4. Caso «Saber v. Noruega» (TEDH, 2020)	99
c) El derecho al anonimato	102
§ 7. Toma de posición y valoración provisoria	104
CAPÍTULO III	
DERECHO PROCESAL PENAL EN LA ERA DIGITAL. EL DERECHO DE DEFENSA EN JUICIO Y LA PROHIBICIÓN DE AUTOINCRIMINACIÓN	
§ 8. La evolución histórica de la prueba y los límites constitucionales para su obtención	109
§ 9. El derecho de defensa enjuicio	111
a) La incorporación al proceso penal de prueba digital proveniente de terminales móviles multiplataforma de convergencia de TIC, sin el procedimiento forense adecuado	114
b) La prueba digital extraída determináñales móviles multiplataforma de convergencia de TIC, mediante sistemas de inteligencia artificial (IA)	116
1. La inteligencia artificial y el sistema de Administración de Justicia	117
I. Cold Case	119
II. Sweetie	119
III. Valeri («Visual Analyticsforsensemaking inCriminal Intelligence analysis»)	120
IV. CompStat	120
V. PredPol	121

VI. NDAS («National Data Analytics Solution»)	121
VII. Veripol	122
VIII. iBorderCtrl	122
IX. Questmap	122
X. Data Mining	123
XI. IBM'sWatson Debater	123
XII. Ross Intelligence	123
XIII. Hart («Harm Assessment Risk Tool»)	124
XIV. Precobs-KrimPro-KLB-PreMap-Skala	124
XV. Compás («Correctional Offender Management Profiling for Alternative Sanctions»)	126
XVI. Sherlock Legal	127
XVII. Prometea	128
XVIII. Sense Time (Sistema de crédito social ciudadano)	130
2. El derecho de defensa en juicio y los programas forenses asistidos por inteligencia artificial (IA) destinados a obtener prueba digital de terminales móviles	132
I. Casos «State v. Loomis» (2016) y «Loomis v. Wisconsin»(2017)	134
II. Caso «Rechtbank Den Haag» (2020)	136
3. Toma de posición sobre el derecho de defensa en juicio y el empleo de programas forenses asistidos por inteligencia artificial (IA) destinados a obtener prueba digital de terminales móviles	138
§ 10. La garantía de prohibición de autoincriminación	146
a) La garantía de prohibición de autoincriminación y el desbloqueo de teléfonos celulares inteligentes («smartphone»)	147
b) Caso «USDC. District of Idaho» (2019)	152
c) Caso «USDC Northern District of California» (2019)	152
d) Caso «Seo v. Indiana State» (2020)	153
e) Caso «United States v. Jones»(2021)	155
f) Toma de posición frente a la prohibición de autoincriminación por entrega de contraseñas, patrón de puntos o datos biométricos de desencriptación de terminales móviles	157
§ 11. Toma de posición y valoración provisoria	159
 CAPÍTULO IV	
LA PRUEBA DIGITAL	
§ 12. La naturaleza de la prueba digital y sus características diferenciales de la prueba física, corpórea o tangible	165
a) El análisis forense informático	170
b) El análisis forense móvil	171
c) Las técnicas forenses de red	172
§ 13. Procedimiento forense básico y común a los tres análisis forenses, informático, móvil y en redes, para la obtención de prueba digital conservando su integridad e Inalterabilidad	173
a) La presencia de un perito especializado en informática forense	174
b) La presencia de un escribano público	174
c) La información extraída debe ser protegida mediante la aplicación de códigos criptográficos en función de «hash»	175
d) Filmar todo el procedimiento	177
e) El labrado de un acta que documente el procedimiento realizado para la obtención de prueba digital	177
f) Completar por parte del perito especializado en informática forense el correspondiente formulario de algoritmo criptográfico utilizado	177
§ 14. El proceso unificado de recuperación de información (PURI)	178
a) Fase nº 1 del PURI. Relevamiento	179
b) Fase nº 2 del PURI. Recolección	180

c) Fase nº 3 del PURI. Adquisición	181
d) Fase nº 4 del PURI. Preparación	182
e) Fase nº 5 del PURI. Extracción y análisis	183
f) Fase nº 6 del PURI. Presentación	183
§ 15. El análisis forense móvil	184
a) La preconstitución de prueba digital proveniente de teléfonos celulares inteligentes («smartphones») o terminales móviles multiplataforma de convergencia de TIC	184
1. Procedimiento de preconstitución de prueba digital proveniente de terminales móviles	185
2. Preconstitución de prueba digital proveniente de terminales móviles mediante herramientas forenses	186
b) La recolección de la prueba digital en el análisis forense móvil	187
1. Fase de recolección del equipo de telefonía móvil	188
— Estados en los que puede encontrarse el equipo de telefonía móvil	189
1.1. Estado de encendido del equipo de telefonía móvil	189
1.2. Estado apagado del equipo de telefonía móvil	189
2. Fase de adquisición. Etapa de embalaje y traslado del equipo de telefonía móvil al laboratorio informático forense	189
c) El peritaje de la prueba digital en el análisis forense móvil	190
d) La conservación de la prueba digital en el análisis forense móvil	193
§ 16. Técnicas forenses en red como complementario del análisis forense móvil	193
a) La prueba digital proveniente de la computación de la nube	194
b) Técnicas para la obtención de prueba digital en la computación de la nube («cloud computing»)	199
1. La estructura de la computación de la nube, o entorno digital distribuido	199
2. Obtención de prueba digital de la nube alojada en el territorio nacional	201
I. Obtención de prueba digital con acceso al RAID pudiendo trasladarse el equipo	201
II. Obtención de prueba digital con acceso al RAID, en los casos en los cuales no es posible trasladar el equipo	202
III. Obtención de prueba digital con acceso al RAID, en los casos en los cuales el equipo está desmontado	203
3. Obtención de prueba digital de la nube situada en extraña jurisdicción	204
I. Acceso a datos abiertos	206
II. Acceso a datos restringidos	207
II.1. Acceso transfronterizo directo a través de una terminal ubicada en la jurisdicción en la que tramita la investigación	207
II.2. Acceso transfronterizo directo mediante mecanismos técnicos	208
II.3. Acceso transfronterizo a través de los proveedores de servidores informáticos u otras empresas por medio de cooperación asimétrica	209
4. Interceptación o captura del tráfico de datos entre el nodo y la nube	210
c) La prueba digital proveniente de la red profunda («deep web»)	210
1. El acceso remoto a la terminal móvil que se conectara a la red profunda (deep web)	214
— Caso «United State v. Levin» (2016)	215
2. La toma del control físico de la terminal móvil multiplataforma de convergencia de TIC	216
§ 17. Toma de posición y valoración provisoria	216
a) Preconstitución de prueba digital obtenida de terminales móviles)	219
b) Peritaje de prueba digital obtenida de terminales móviles	221
c) Conservación de prueba digital obtenida de terminales móviles	224
d) Prueba digital obtenida de la nube cuando la terminal móvil es utilizada como plataforma de acceso a la nube	224

e) Prueba digital obtenida de la red profunda por medio de una terminal móvil como plataforma de acceso	226
CAPÍTULO V	
LA PRUEBA DIGITAL EN LA LEGISLACIÓN NACIONAL Y PROVINCIAL	
§ 18. El Convenio de Ciberdelincuencia de Budapest de 2001 (ley 27.411)	228
§ 19. Antecedentes nacionales en materia de regulación de la criminalidad informática	230
§ 20. La reforma al Código Penal en materia de criminalidad informática (leyes 26.388, 26.904 y 27.436)	231
§ 21. La prueba digital en los códigos procesales penales federales	237
a) Código Procesal Penal de la Nación (ley 23.984)	237
b) Código Procesal Penal Federal (ley 27.063 y modificaciones ley 27.482)	238
§ 22. Los códigos procesales provinciales que regularon la prueba digital	240
a) Código Procesal Penal de la Ciudad Autónoma de Buenos Aires (ley 2303, ordenada por ley 2452 y modificada por la ley 6017)	240
b) Código Procesal Penal de la Provincia de Corrientes (ley 6518)	243
c) Código Procesal Penal de la Provincia de Neuquén (ley 2784)	249
d) Código Procesal Penal de la Provincia de Río Negro (ley 5020)	252
e) Código Procesal Penal de Tucumán (ley 8933)	253
§ 23. Los códigos procesales provinciales que no regularon aún la prueba digital	259
a) Código Procesal Penal de la Provincia de Buenos Aires (ley 11.922)	259
b) Código Procesal Penal de la Provincia de Catamarca (ley 5097)	259
c) Código Procesal Penal de la Provincia de Chaco (ley 4538)	260
d) Código Procesal Penal de la Provincia de Chubut (ley 5478)	260
e) Código Procesal Penal de la Provincia de Córdoba (ley 8123)	261
f) Código Procesal Penal de la Provincia de Entre Ríos (ley 9754)	262
g) Código Procesal Penal de la Provincia de Formosa (ley 696)	262
h) Código Procesal Penal de la Provincia de Jujuy (ley 5623)	263
i) Código Procesal Penal de la Provincia de La Pampa (ley 332)	263
j) Código Procesal Penal de la Provincia de La Rioja (ley 8774)	264
k) Código Procesal Penal de la Provincia de Mendoza (ley 6730)	264
l) Código Procesal Penal de la Provincia de Misiones (ley 14)	267
m) Código Procesal Penal de la Provincia de Salta (ley 7690)	267
n) Código Procesal Penal de la Provincia de San Juan (ley 1851)	268
ñ) Código Procesal Penal de la Provincia de San Luis (ley 5724)	269
o) Código Procesal Penal de la Provincia de Santa Cruz (ley 2424)	269
p) Código Procesal Penal de la Provincia de Santa Fe (ley 12.734)	270
g) Código Procesal Penal de la Provincia de Santiago del Estero (ley 6941)	270
r) Código Procesal Penal de la Provincia de Tierra del Fuego (ley 168)	270
§ 24. Toma de posición y valoración provisoria	271
CAPÍTULO VI	
LA PRUEBA DIGITAL OBTENIDA DE TERMINALES MÓVILES EN LA LEGISLACIÓN EXTRANJERA	
§ 25. La república federal de Alemania	278
a) Vigilancia de telecomunicaciones («Telekommunikationsüberwachung», § 100a, StPO)	280
b) Búsqueda en línea («Online-Durchsuchung», § 100b, StPO)	288
c) Recopilación de datos de tráfico («Erhebung von Verkehrsdaten», § 100g, StPO)	293
d) Técnica de investigación en terminales móviles. («Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten», § 100i, StPO)	295
§ 26. El reino de España	299
a) Disposiciones comunes	301
b) La interceptación de las comunicaciones telefónicas y telemáticas	306

c) Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos	313
d) Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización	317
e) Registro de dispositivos de almacenamiento masivo de información	321
f) Registros remotos sobre equipos informáticos	325
g) Medidas de aseguramiento	329
§ 27. Los Estados Unidos de América	330
a) Búsqueda e incautación de evidencia digital	330
b) Búsqueda de evidencia digital en otra jurisdicción	333
c) Destrucción de evidencia digital	336
d) La jurisprudencia estadounidense en torno a la obtención de prueba digital de terminales móviles	336
§ 28. Japón	339
§ 29. Toma de posición y valoración provisoria	342
 CAPÍTULO VII	
LA CORRECTA OBTENCIÓN DE PRUEBA DIGITAL DE TERMINALES MÓVILES	
MULTIPLATAFORMA DE CONVERGENCIA DE TIC	
§ 30. La terminal móvil multiplataforma de convergencia de TIC	351
§ 31. La obtención de prueba digital por medio del registro de la terminal móvil como dispositivo electrónico de almacenamiento masivo de información	353
§ 32. La obtención de prueba digital por medio de la vigilancia o interceptación de telecomunicaciones electrónicas de la terminal móvil	359
§ 33. La obtención de prueba digital a través del acceso remoto a la terminal móvil	364
a) La obtención de prueba digital de la computación de la nube («cloud computing»)	367
b) La obtención de prueba digital de información almacenada en la red profunda («deep web»)	368
c) Procedimiento de obtención de prueba digital a través de acceso remoto a la terminal móvil	369
§ 34. La obtención de prueba digital a través del empleo de la terminal móvil como dispositivo de vigilancia acústica	372
§ 35. La obtención de prueba digital a través del empleo de la terminal móvil como dispositivo de seguimiento y localización	376
 CAPÍTULO VIII	
CONCLUSIONES	
FUENTES Y BIBLIOGRAFÍA	381
	395