

ÍNDICE GENERAL

ABREVIATURAS	17
---------------------------	----

CAPÍTULO I

LAS COMUNICACIONES POR WHATSAPP COMO PRUEBA EN JUICIO

§ 1. “Protección expansiva” y “amplitud probatoria”, una difícil convivencia	21
§ 2. Conversaciones mantenidas por WhatsApp. Introducción	24
§ 3. Marco de regulación en el Código Procesal Federal	26
a) Libertad probatoria	26
b) Responsabilidad probatoria	26
c) Interceptación de correspondencia	27
d) Incautación de datos	27
e) Síntesis	27
§ 4. Regulación en las provincias argentinas	28
a) Libertad probatoria	28
b) Responsabilidad probatoria	29
c) Interceptación de correspondencia	29
d) Intervención telefónica	30
e) Incautación de datos. Registro remoto	30
f) Síntesis	31
§ 5. Los mensajes de WhatsApp como medio de prueba	31
a) Legalidad de origen	32
b) Naturaleza de la evidencia	33
c) Valor probatorio	34
d) Posibilidad de adulteración, alteración y manipulación de los mensajes	34
e) Acceso a conversaciones futuras	35
f) “Pantallazos” de WhatsApp. Prueba real y demostrativa	37
1. Caracteres de la evidencia demostrativa y real	40

2. Representación <i>versus</i> autenticación	41
3. Forma de utilización de la evidencia	41
4. Introducción del pantallazo de WhatsApp en juicio	43
g) Carga de autenticación de las conversaciones por WhatsApp	43
h) Uso de conversaciones por WhatsApp. Litigación con perspectiva de género ..	44
i) Los mensajes de WhatsApp en la etapa de investigación	45
j) Los mensajes de WhatsApp en la etapa de admisión de evidencias	46
— A modo de síntesis	48
k) Los mensajes de WhatsApp en el juicio	50
l) WhatsApp. Test de autenticación. Estándar de prueba	51
m) Objeción al ingreso de información proveniente de WhatsApp	57
n) Ausencia de integralidad como objeción al ingreso de la comunicación	58
ñ) Omisión de indefensión y admisión de pruebas	60
o) Los desafíos que impone el uso de WhatsApp en juicio	61
1. Necesidad de abandonar viejas prácticas	61
2. Autenticación y valoración. Dos caras de la misma moneda	61
3. Amplitud probatoria	62
4. Litigación en contexto de género	62
§ 6. Jurisprudencia vinculada	63
a) Jurisprudencia local	63
1. ¿Son válidas las capturas de pantallas transcritas?	63
2. ¿El uso de mensajes como prueba viola el derecho a la intimidad?	64
3. Conversaciones y capturas aportadas por el denunciante	66
I. Los hechos	66
II. Pedido de nulidad	67
III. Solución del caso	67
4. ¿Son legales las grabaciones efectuadas entre particulares?	70
5. ¿La filmación en el domicilio podría afectar la intimidad?	72
6. ¿Se puede utilizar una conversación con el propósito de denunciar al inter- locutor?	73
7. ¿Es legal escuchar la conversación ajena?	73
8. Grabaciones de conversaciones y capturas aportadas voluntariamente ..	74
9. Amenaza por WeChat. Violencia de género	75
I. Solución del caso	76
II. Calificación legal	77
10. A modo de síntesis	78
b) Jurisprudencia del Reino de España	79
1. Introducción	79
2. Jurisprudencia destacada	79
I. Legalidad	79
II. Carga de autenticación	80
III. Intervención de un notario	81
IV. Naturaleza jurídica del “pantallazo”. Autenticación	81
V. Pantallazo de WhatsApp. Falta de autenticación. Prueba ilícita	84
VI. Ausencia de presunción contraria a la autenticidad	88

VII. WhatsApp. Ausencia de pericia. Prueba por otros medios	90
VIII. WhatsApp. Pantallazos. Exhibición a terceros. Legalidad	92
IX. Silencio del acusado respecto de las imágenes	93
X. Mensajería de Facebook	94
XI. Mensajería. Redes sociales. Tribunal Supremo de Galicia	95
3. Síntesis de la jurisprudencia española	95
c) Jurisprudencia de Colombia	96
1. Introducción	96
2. Prueba electrónica. Alcances	96
3. WhatsApp. Naturaleza	97
4. WhatsApp. Valor probatorio	97
5. Capturas de pantalla. Indicio	98
6. Captura de pantalla. Naturaleza	98
7. WhatsApp. Autenticidad	99
8. Síntesis	99
9. Valoración de mensajes de WhatsApp. Equiparación a documentos	100

CAPÍTULO II

**IDENTIFICACIÓN Y DESBLOQUEO DEL CELULAR.
LA SOCIEDAD EN LA ERA DE LAS CONTRASEÑAS**

§ 7. ¿El teléfono móvil es parte de la anatomía humana?	103
§ 8. La sociedad en la era de las contraseñas	107
§ 9. Teléfono celular. Identificación, seguimiento, consentimiento y desbloqueo forzoso	110
a) Identificación y vinculación del celular con una persona	112
b) Seguimiento y reconstrucción	113
c) Localización	114
d) Identificación del celular robado o extraviado	114
e) Búsqueda de datos internos. Desbloqueo	115
1. Consentimiento del titular	116
2. Consentimiento prestado por terceras personas	118
I. Uso común	119
II. Dispositivo usado por un menor	120
III. Dispositivo adquirido por la pareja	121
IV. Dispositivos usados en el ámbito laboral	122
3. Consentimiento prestado por “bloques de información”	122
4. Consentimiento, orden judicial	122
I. Hallazgos casuales y de buena fe	122
II. Hallazgos inevitables. Extralimitación en la orden. Excursión de pesca	126
5. ¿El consentimiento para registrar un domicilio se extiende al registro del teléfono?	127
f) ¿Puede utilizarse un dato expuesto a simple vista?	128

g) Desbloqueo. Utilización forzosa del patrón biométrico obtenido del rostro, iris o huella dactilar	129
1. Tesis amplia: acepta el desbloqueo. Orden judicial fundada	129
2. Tesis restrictiva. Acepta el desbloqueo. Fija condiciones	131
h) Exigencia de entregar, insertar o dictar la clave del teléfono celular	132
i) Desbloqueo forzoso. Toma de posición	133
1. Uso de datos biométricos. Orden de revelar, entregar o ingresar la clave	135
2. Solicitud de la orden judicial	136
3. Orden judicial fundada	136
4. Fundamentos de la orden judicial	139
5. Excursión de pesca. Hallazgo casual. Análisis previo y posterior	140
6. Hallazgo casual en el marco de un Allanamiento. Práctica	150
7. Tipos de hallazgos casuales. Investigación. Excursión de pesca	151
§ 10. ¿Por qué el uso forzoso de datos biométricos para desbloquear el teléfono celular no es autoincriminatorio?	154
a) No son testimoniales	155
b) Acceso al celular, no a su contenido. Privacidad, no autoincriminación	157
c) Testimonial implícita. Conclusión inevitable	161
d) Expectativa razonable de privacidad <i>versus</i> expectativa razonable de impunidad	162
§ 11. Acceso al celular. Urgencia. Pérdida de información vital	167
a) Acceso al celular. Urgencia. Peligro para los agentes	170
b) Protocolo federal. Primera intervención en dispositivos móviles y celulares	170
c) Intervención de acuerdo a lo dispuesto por la autoridad judicial	173
d) Secuestro de cargador, cables y datos	174
e) Aporte de información espontánea. Documentación	174
f) Preservación del dispositivo	174
g) Diez preguntas que deben responderse a la hora de testear una orden de desbloqueo	176
h) Desbloqueo. Casos prácticos. Requisitos	177
1. Conductor sospechoso	177
2. Allanamiento de vivienda. Secuestro de celulares. Otros dispositivos. ¿Acceso?	179
§ 12. Desbloqueo forzoso. Jurisprudencia	181
a) Jurisprudencia argentina	181
1. Desbloqueo forzoso	181
I. Los hechos del caso	182
II. Planteo de la defensa	182
III. Respuesta fiscal	183
IV. Análisis de la Cámara	183
IV.1. Necesidad y proporcionalidad de la medida	183
IV.2. Legalidad de la medida	184
IV.3. ¿Puede solicitarle a la sospechada los datos biométricos?	185
IV.4. Solución del caso	186
2. Obtención de una copia de los datos almacenados en el celular	187
I. El caso	187

II. Acceso al teléfono con el fin de obtener una copia	187
III. Ausencia de norma. Aplicación de la ley 27.063	188
IV. Cadena de custodia. Valor probatorio	189
V. Falta de perjuicio concreto	190
VI. Convalidación	190
3. Delito. Ingreso al celular de la pareja	190
4. Acceso sin consentimiento al celular de la hija	192
5. ¿Es posible desbloquear utilizando la huella digital de un cadáver?	194
b) Jurisprudencia de los Estados Unidos de América	195
1. Acceso al celular y sus datos en la jurisprudencia de los Estados Unidos de América	195
I. Contexto y evolución	196
II. Análisis de los precedentes	199
II.1. "Olmstead v. United States"	199
II.2. "Goldman v. United States". Interceptación real	200
II.3. "Katz v. United States". Ampliación del concepto de privacidad	200
II.4. "Smith v. Maryland". Expectativa razonable de privacidad	202
II.5. "Riley v. California". Inspección del celular sin orden judicial	206
II.6. "Carpenter v. United States". Acceso a la información generada por el uso del celular	210
2. Casos sobre desbloqueo y descifrado forzoso	222
I. Orden de desbloquear el iPhone. Negativa. Desacato. Autoincriminación. "Katelin Eujoo Seo v. Indiana State"	222
I.1. Los hechos	222
I.2. Obligación de aportar la clave del celular. Autoincriminación	223
I.3. Síntesis. Desbloqueo. Acceso a la información	226
3. Orden de desbloquear el teléfono celular incautado. Requisitos. Autoincriminación	226
I. Los hechos del caso	227
II. Apelación de la orden de desacato	228
III. Corte Suprema. Revoca orden de desacato	228
4. Orden judicial de proveer la clave o descifrar archivos	229
I. Orden judicial que exige descifrar archivos secuestrados. Viola la V Enmienda	230
II. Orden que exige proporcionar la contraseña de acceso a la computadora. Viola la V Enmienda	232
5. Orden de entregar la contraseña del teléfono y desbloquearlo con la huella digital	233
6. Obligación de insertar la clave de desbloqueo. "Commonwealth v. León Gelfgatt", SJC-11358. Suffolk, Noviembre 5, 2013 - June 25, 2014	234
7. Desbloqueo forzoso. Uso de huellas dactilares. "State of Minnesota v. Matthew Vaughn Diamond", A15-2075 (2018)	236
I. Los hechos del caso	236
II. Solicitud de desbloqueo. Oposición del sospechoso	237
III. Resolución del juez	237

IV. Uso de la evidencia obtenida en juicio. Condena	237
V. Revisión de la condena	238
V.1. Privilegio contra la autoincriminación forzosa	238
V.2. Respeto por la dignidad e integridad humana	239
V.3. Carga de la prueba	239
V.4. Extensión del privilegio contra la autoincriminación forzada	240
V.5. Declaración testimonial. Alcances	240
V.6. Obtención forzada de la huella digital para desbloquear el celular	242
8. Acceso al celular. Consentimiento prestado por la esposa. Persona detenida	244
—. Los hechos del caso	244
—. Solución del TSPR	246
a. Necesidad de contar con una orden judicial	246
b. Excepciones a contar con una orden judicial	246
c. El consentimiento como autorización de registro	247
d. Examen del consentimiento. Ambiente	247
e. Consentimiento prestado por terceras personas	248
9. Síntesis. Desbloqueo y descifrado forzoso en los Estados Unidos de Norteamérica	251
10. Conclusión	253
11. Posturas en contra del desbloqueo forzoso mediante orden judicial	254
c) Jurisprudencia. Reino de España	258
1. Acceso al celular y sus datos en la jurisprudencia de España	258
2. Constatación de contactos telefónicos sin orden judicial	258
3. Apertura de agenda física y acceso a un ordenador	261
4. Acceso a llamadas entrantes y salientes de un celular	262
5. Indagación en datos del celular	262
6. Derecho a un entorno digital. Acceso a un «smartphone»	264
7. Acceso a los datos que contiene el celular. Orden judicial	264
d) Jurisprudencia de México	271
1. El medio que protege	272
2. Qué protege	273
3. Divulgación entre comunicantes	274
4. Prueba ilícita. Protección entre particulares	274
5. Alcance temporal de la protección	275
6. Datos que identifican la comunicación	276
7. Síntesis de los presupuestos	276
8. Conclusión	278

CAPÍTULO III

**LA INVESTIGACIÓN PENAL EN LA ERA DIGITAL.
CASUÍSTICA**

§ 13. Prueba digital	281
a) Introducción	281

b) Análisis de casos conflictivos	282
1. Registro de una computadora en el interior de un domicilio	282
2. El secuestro de las computadoras para registro	286
3. Acceso a los datos internos del celular secuestrado	288
4. Registro remoto de una computadora y otros dispositivos	290
5. Hallazgos casuales durante un registro en la computadora	296
6. Orden judicial de registro. Consentimiento. Hallazgo casual. Límites	296
7. Acceso a «todos» los archivos durante el registro	299
8. Autorización a acceder a un equipo y sus datos en la «nube»	300
9. El espionaje informático	301
10. Registro urgente de un celular secuestrado	302
11. Consentimiento para el registro del celular	303
12. Intervención de un celular sustraído	304
13. Intervención de un celular con titular desconocido	304
14. Intervención de celulares de terceras personas	305
15. Secuestro del celular a quien toma fotos de un accidente	305
16. Intervención de un teléfono público	308
17. Escucha y grabación de comunicaciones entre presentes	308
18. Grabación de un soborno a un funcionario	313
19. Obligación de entregar la clave del celular	315
20. Información obtenida por el agente provocador y agente encubierto	315
21. Agente encubierto, provocador y revelador en Internet	320
22. «Grooming». Entrampamiento del agresor por parte de particulares	323
23. Ciberpatrullaje. Prevención de delitos. El patrullaje en la red	324
24. Acceso a datos, fotos, videos y ficheros	325
25. Información obtenida de muros. Twitteos	326
26. Publicaciones como prueba de refutación	329
27. Orden de conservación de datos	330
28. Información sobre el titular de la línea telefónica	330
29. Acceso a correos electrónicos	330
30. Mensajes de texto, «chats», mensajería electrónica	332
31. Recuperación de información de la computadora o celular	333
32. Recuperación de registros obtenidos de un dispositivo descartado, abandonado	333
33. Grabación subrepticia de voz en comisaría	333
34. Rastreo de dirección IP	334
35. Rastreo del IMEI	334
36. Acceso a datos de comunicación conservados por terceros	337
37. Listados de llamadas entrantes y salientes	339
38. Utilización de scanner en la intervención telefónica	340
39. Uso de un teléfono asumiendo la identidad del sospechoso	340
40. Escuchas y videofilmaciones en las cárceles	342
41. Conversaciones, el «chat» ¿sitio privado o público?	345
42. Fotos y videos en el «chat»	347
43. Búsqueda y publicaciones en Facebook realizadas por la víctima para intentar contactar a los sospechosos	349
44. Identificación digital del sospechoso. ¿Reconocimiento virtual?	351

45. Comunicaciones por radiofrecuencia	353
46. Colocación de micrófono o dispositivo de seguimiento en un vehículo	353
47. Secreto en las fuentes periodísticas	355
48. Grabaciones con propósito de denunciar al interlocutor	355
49. Grabación de conversaciones autoincriminatorias	355
50. Captación de conversaciones de terceros para difusión	357
51. Colocar un GPS en un paquete postal	358
52. Cámara oculta	359
53. Cámaras ocultas en programas de televisión	360
54. Derecho a la propia imagen y derecho a informar	362
55. Grabación de imagen y sonido en lugares públicos y privados	363
56. El seguimiento de sospechosos en la vía pública	365
57. Grabación de conversaciones con el abogado	366
58. Acceso a los archivos de una computadora dejada en el «service»	369
I. Previsión legal	371
II. Urgencia	372
III. Fin legítimo	373
59. Localización del celular a partir de antenas falsas	375
60. Incautación del teléfono en un arresto. Hallazgo a simple vista	376
61. «Chat» de un mayor con una supuesta menor con fines sexuales. Ausencia de entrampamiento	376
62. Acceso a una computadora utilizada en el trabajo	378
63. Monitoreo de las comunicaciones en el lugar de trabajo	379
64. Acceso a los correos electrónicos para investigar la conducta de la empleada	381
65. Utilización de una cuenta laboral con fines particulares	382
66. Obtención de material de la computadora que utiliza un empleado en el tra- bajo	384
67. Filmaciones en el lugar de trabajo	385

CAPÍTULO IV

HABILIDADES Y DESTREZAS EN LA PREPARACIÓN DE UN CASO CON EVIDENCIA DIGITAL

§ 14. Introducción	387
§ 15. La prueba digital en la era de la distracción	387
§ 16. Diez sugerencias para diseñar una estrategia adecuada para el ingreso de evidencia digital	390
a) Litigue estratégicamente. Elija qué información presentar	390
b) Elija el jurado amigable con las nuevas tecnologías. «Voir dire»	393
c) Mantenga el dominio. Conozca la prueba	395
d) Acredite al experto. Prepare el examen	397
e) No complique lo simple. Examen al investigador	399
f) No se deje estar. Advierta eventuales objeciones	400
g) Evite sorpresas. Instale la familiaridad con la prueba	400
h) No sume tiempo restando atención. Use el tiempo de modo adecuado	401

ÍNDICE GENERAL

15

<i>i)</i> Verifique antes de usar. Chequee las cuestiones técnicas	402
<i>j)</i> No dé nada por sentado. Trabaje el frente y los flancos	404
§ 17. A modo de síntesis. Manténgase en juego	405
§ 18. Jurado popular. Prueba digital y demás factores que inciden en la toma de decisión	407
§ 19. Anatomía de un veredicto. Diagrama	415

CAPÍTULO V

ÉTICA Y PRUEBA DIGITAL

§ 20. Redes sociales. Instrucciones al jurado. Mala conducta digital	418
§ 21. Juicio justo. Influencia digital. ¿Secuestro virtual?	426
§ 22. ¿Pueden los abogados alegar más allá de la evidencia rendida en juicio?	428

BIBLIOGRAFÍA GENERAL	431
-----------------------------------	-----