ÍNDICE GENERAL

PRÓLOGO ____ 13
INTRODUCCIÓN ____ 19
ABREVIATURAS ____ 27

CAPÍTULO I
¿QUÉ SON LOS METADATOS, PARA QUÉ SIRVEN Y CÓMO SE LOS PUEDE INCORPORAR AL PROCESO PENAL?

§ 1. Introducción ____ 29
§ 2. La regulación de los metadatos en la Argentina ____ 32
§ 3. Los metadatos en la doctrina y la jurisprudencia norteamericanas ____ 37
a) Dicotomía público/privado ____ 39
b) "Third-party doctrine" (información secreta/compartida) ____ 42
c) Información considerada "contenido" versus información considerada "sin contenido" ____ 45
§ 4. Aplicación de las tres dicotomías a los metadatos ____ 48
a) El argumento de la neutralidad tecnológica ____ 48
b) La aplicación de la "third-party doctrine" a los metadatos y la alegada ausencia de expectativa de privacidad ____ 50
c) Los metadatos son "información sin contenido" ____ 52
d) Jurisprudencia norteamericana que establece que los metadatos, en la era digital, no deben contar con protección constitucional ____ 53
§ 5. Los metadatos y el derecho a la intimidad ____ 56
a) Los metadatos pueden revelar información privada sobre nosotros ____ 57
b) ¿Son los metadatos "información sin contenido"? ____ 59
c) La "third-party doctrine" y los metadatos ____ 60
d) Cambio de criterio en la jurisprudencia norteamericana ____ 64
§ 6. Conclusiones ____ 68

CAPÍTULO II

DESBLOQUEO DE TELÉFONOS CELULARES A TRAVÉS DEL INGRESO COMPULSIVO DE DATOS BIOMÉTRICOS

§ 7. Introducción ____ 73
§ 8. Encriptación ____ 77
§ 9. Jurisprudencia norteamericana sobre el desbloqueo de teléfonos celulares mediante el ingreso compulsivo de datos biométricos de sus usuarios ____ 80
§ 10. Jurisprudencia argentina sobre el uso del cuerpo del imputado como fuente de evidencia ____ 86
§ 11. El desbloqueo de teléfonos celulares mediante el ingreso compulsivo de datos biométricos del imputado ____ 88
§ 12. El contenido testimonial implícito en el ingreso compulsivo de datos biométricos ____ 90
§ 13. "Foregone conclusion" y la posibilidad de requerir el ingreso compulsivo de datos biométricos para desbloquear un teléfono celular sin violar la garantía contra la autoincriminación ____ 95
§ 14. Conclusiones ____ 97

CAPÍTULO III

UNA CUESTIÓN DE CÓDIGOS: LA UTILIZACIÓN DE ALGORITMOS SECRETOS EN LA JUSTICIA PENAL

§ 15. Introducción ____ 99
§ 16. Nuevas técnicas forenses para obtener evidencia: la aparición de los algoritmos en la justicia penal ____ 104
a) Técnicas forenses de primera y segunda generación ____ 104
b) Códigos fuente ____ 107
c) Programas forenses que se utilizan en la justicia penal ____ 110
1. UFED ____ 110
2. Encase ____ 111
3. TrueAllele ____ 111
4. Programas de detección de alcohol en aliento ____ 112
5. Programas de reconocimiento facial ____ 113
6. ShotSpotter ____ 113
7. Dispositivo Stingray ____ 114
8. Compas ____ 115
d) Ventajas de la utilización de estas nuevas tecnologías en el sistema penal ____ 116
e) Críticas a la utilización de las técnicas forenses de segunda generación ____ 117
f) Algoritmos secretos ____ 119
g) Errores en los algoritmos ____ 120
§ 17. Jurisprudencia de Estados Unidos con relación a la incorporación de evidencia obtenida a través de nuevas técnicas forenses ____ 125
a) El caso "Frye". Los criterios para admitir evidencia obtenida a través de métodos novedosos ____ 125

b) El caso "Daubert" y los requisitos para admitir evidencia obtenida a través de nuevas técnicas forenses/científicas ____ 126
c) El caso "Kumho Tire Company". La irrelevancia del adjetivo "científico" y los criterios para evaluar la confiabilidad de la evidencia ____ 128
d) "United States v. Ocasio": una excepción al criterio general ____ 130
e) TrueAllele y el privilegio del secreto empresarial. El caso "The People v. Chubbs" 130
f) FST. Las consecuencias de la falta de publicidad del código fuente en programas de análisis de ADN. Los casos "People v. Carter" y "United States v. Johnson" ____ 135
g) La utilización de Compas para la determinación de la pena. El caso "State v. Loomis" ____ 137
h) Stingray y ShotSpotter: posibles violaciones a derechos constitucionales ____ 140
i) El estado actual del conflicto y su posible impacto en la Argentina ____ 142

§ 18. Posibles soluciones al problema de los algoritmos secretos ____ 144
a) Los fallos "Daubert" y "Kumho Tire" en Estados Unidos. Los jueces como guardianes ____ 144
b) Aplicación del estándar de "Daubert" en la justicia argentina ____ 146
c) Conclusiones: la aplicación de "Daubert" a los programas con algoritmos secretos 148
d) "Bonus track": ¿qué hacer con los programas predictivos del estilo de Compas? 153

CAPÍTULO IV

ANÁLISIS DE INFORMACIÓN CONTENIDA EN DISPOSITIVOS DE ALMACENAMIENTO DIGITAL: EL PROBLEMA DE LA APLICACIÓN DE LA «PLAIN VIEW DOCTRINE» A ENTORNOS DIGITALES

§ 19. Introducción ____ 157
§ 20. Principios generales que rigen los allanamientos en el mundo físico y la "plain view doctrine". El problema de aplicarlos al entorno digital ____ 160
a) Allanamiento y "plain view doctrine" en el mundo físico ____ 160
b) Dificultades en el análisis de archivos en entornos digitales ____ 165

§ 21. Análisis de información resguardada en dispositivos de almacenamiento digital ____ 167
a) Modo en que tradicionalmente se secuestra y analiza información almacenada digitalmente ____ 167
b) El análisis digital. Limitaciones "ex ante" versus análisis de la razonabilidad del desarrollo de la medida "ex post" ____ 171
1. Jurisprudencia norteamericana que impone límites "ex ante" al análisis de información resguardada en dispositivos de almacenamiento digital ____ 173
I. Límites al "hardware" que se puede secuestrar ____ 173
II. Límites al tiempo en que se puede analizar información digitalmente almacenada ____ 175
III. Obligación de observar protocolos que estructuran cómo se deben desarrollar las búsquedas de información digital relevante ____ 177
IV. Condición de devolver los elementos secuestrados dentro de un plazo determinado ____ 183

2. Críticas a la imposición de restricciones "ex ante" _____ 183
I. Críticas a la imposición de restricciones "ex ante" desde la perspectiva constitucional norteamericana _____ 183
II. Críticas a la imposición de restricciones "ex ante" desde la perspectiva de la practicidad _____ 185
II.1. Críticas a los límites respecto del "hardware" que se puede secuestrar y del tiempo para practicar el análisis de la información digital recolectada _____ 186
II.2. Críticas a la imposición de protocolos de análisis y a la necesidad de devolver los efectos en un corto plazo _____ 187

§ 22. Evaluación "ex post" de la razonabilidad del modo en que se ejecuta el análisis de información digital y aplicación de la "plain view doctrine" _____ 189
§ 23. Críticas a la aplicación de la "plain view doctrine" al entorno digital _____ 194
§ 24. Propuestas alternativas a la utilización de la "plain view doctrine" en el entorno digital _____ 198
§ 25. Conclusiones: el uso de restricciones como forma de medir la razonabilidad del análisis de información en entornos digitales _____ 201

CAPÍTULO V

EL DERECHO A QUE SE ELIMINE LA INFORMACIÓN DIGITAL SECUESTRADA NO RELEVANTE PARA LA INVESTIGACIÓN

§ 26. Introducción _____ 213
§ 27. El caso "United States v. Ganias" y ¿el derecho a eliminar los datos digitales secuestrados que no revisten interés para la investigación? _____ 220
— ¿Qué nos queda de "United States v. Ganias"? _____ 224

§ 28. Protección constitucional de imágenes forenses _____ 225
a) ¿La obtención de una imagen forense debe estar protegida constitucionalmente? 225
b) Alcances de la protección constitucional de las imágenes forenses _____ 232
1. Prohibición de utilizar las imágenes forenses una vez concluida su revisión y excepciones _____ 233
2. Prohibición de generar copias de las imágenes forenses sin autorización judicial 240

§ 29. Conclusiones y la necesidad de legislación que regule el problema _____ 242

ANEXO

ÍNDICE DE FALLOS CITADOS

I. **Jurisprudencia nacional** _____ 245
II. **Jurisprudencia internacional** _____ 246

BIBLIOGRAFÍA GENERAL _____ 249