

## ÍNDICE GENERAL

<b>PALABRAS PREVIAS A LA SEGUNDA EDICIÓN</b> .....	15
<b>AGRADECIMIENTOS</b> .....	17
<b>PRÓLOGO DE MARCELO A. RIQUERT</b> .....	23
<b>PRÓLOGO DE MARCOS SALT</b> .....	27
<b>ABREVIATURAS</b> .....	31
<b>INTRODUCCIÓN</b> .....	33

### CAPÍTULO I

#### **LA ERA DIGITAL**

DE LA SOCIEDAD ANALÓGICA DEL SIGLO XX  
A LA SOCIEDAD DE LA INFORMACIÓN DEL SIGLO XXI  
Y LA REVOLUCIÓN DIGITAL

.....	37
-------	----

### CAPÍTULO II

#### **LA NECESIDAD DE REGULACIÓN NORMATIVA DE LA PRUEBA DIGITAL**

.....	47
-------	----

### CAPÍTULO III

#### **LA PRUEBA DIGITAL**

§ 1. La preconstitución de prueba digital .....	62
a) Preconstitución de prueba sobre un correo electrónico ( <i>e-mail</i> ) .....	62
1. Preconstitución física de la evidencia digital sobre un correo electrónico	63
2. Preconstitución electrónica de la evidencia digital sobre un correo electrónico .....	63

b) Preconstitución de prueba en teléfonos celulares inteligentes ( <i>smartphones</i> )	65
— Preconstitución electrónica sobre un teléfono celular inteligente ( <i>smartphone</i> )	66
I. Veracidad del procedimiento	66
II. Preconstitución de prueba digital sobre un teléfono celular inteligente ( <i>smartphone</i> ), mediante herramientas forenses	68
c) Preconstitución de prueba sobre imágenes digitales	69
1. Preconstitución física de la evidencia digital sobre imágenes digitales	69
2. Preconstitución electrónica de la evidencia digital sobre imágenes digitales	70
d) Preconstitución de prueba en redes sociales (Facebook, MySpace, Sonico, Hi5, Orkut, Haboo Hotel, LinkedIn, Instagram)	71
1. Preconstitución física de la evidencia digital sobre redes sociales	71
2. Preconstitución electrónica de la evidencia digital sobre redes sociales	72
e) Preconstitución de prueba en la computación en la nube ( <i>cloud computing</i> )	73
1. La estructura de la computación de la nube, o entorno digital distribuido	79
2. Obtención de prueba digital de la nube alojada en el territorio nacional	81
I. Obtención de prueba digital con acceso al RAID pudiendo trasladarse el equipo	82
II. Obtención de prueba digital con acceso al RAID, en los casos en los cuales no es posible trasladar el equipo	82
III. Obtención de prueba digital con acceso al RAID, en los casos en los cuales el equipo esta desmontado	84
3. Obtención de prueba digital de la nube situada en extraña jurisdicción	85
I. Acceso a datos abiertos	87
II. Acceso a datos restringidos	89
II.1 Acceso transfronterizo directo a través de una terminal ubicada en la jurisdicción en la que tramita la investigación	89
II.2 Acceso transfronterizo directo mediante mecanismos técnicos	90
II.3 Acceso transfronterizo a través de los proveedores de servidores informáticos u otras empresas por medio de cooperación asimétrica	91
III. Interceptación o captura del tráfico de datos entre el nodo y la nube	92
f) Preconstitución de prueba digital mediante detección de noticias falsas («fake news»)	92
1. Las noticias falsas («fake news»)	92
2. Técnicas de detección de «fake news» y preconstitución de prueba digital	95
I. Protocolo de la IFLA (International Federation of Library Associations and Institutions) para detección temprana de «fake news»	96
I.1 Estudio de la fuente	96
I.2 Leer más allá	96
I.3 Determinar quién es el autor	96
I.4 Búsqueda de fuentes adicionales de información	96
I.5 Comprobación de la fecha de publicación de la noticia	96
I.6 Cerciorarse que no se trate de una broma o sátira	96
I.7 Considerar el sesgo de la publicación	96
I.8 Consultar a un experto	97
II. Detección de «trolls» o «bots» en la creación y difusión de «fake news»	97
II.1 Radio de seguimiento o acción	97

## ÍNDICE GENERAL

11

II.2 Cadencia de tipo o intensidad de publicación	98
II.3 Perfil del usuario	98
II.4 Imagen del perfil del usuario	98
II.5 Identificación o mapeo de propiedades	98
III. Empleo de aplicaciones (APPS) o herramientas automatizadas para detectar «trolls» o «bots» en la creación o difusión de «fake news»	98
g) Preconstitución de prueba digital mediante la detección de falsificaciones profundas («deep fake»)	99
1. Las falsificaciones profundas («deep fake»)	99
2. Técnicas de detección de «deep fake» y preconstitución de prueba digital	101
I. Técnicas forenses de detección de falsificación profunda («deep fake»)	102
I.1 Parpadeo	102
I.2 Diferentes cuerpos	103
I.3 Videos breves o clips cortos	103
I.4 Ausencia de sonido o audio	103
I.5 Clips increíbles	104
II. Empleo de aplicaciones (APPS) o herramientas automatizadas para detectar «deep fake»	104
II.1 Truepic	104
II.2 Serelay	107
§ 2. La pericia sobre la prueba digital	108
§ 3. La preservación del medio de prueba digital	113

### CAPÍTULO IV

## LA VIGILANCIA ELECTRÓNICA

EL PANÓPTICO DIGITAL EN LA SOCIEDAD DE LA INFORMACIÓN

Y LA VIGILANCIA

117

### CAPÍTULO V

## LA VIGILANCIA ELECTRÓNICA

### EN LOS CÓDIGOS

### PROCESALES PENALES

§ 1. La vigilancia electrónica como morigeración de la prisión preventiva (art. 177, inc. i, ley 27.063)	131
§ 2. La implementación de la vigilancia electrónica en el vigente Código Procesal Penal de la Nación (ley 23.984)	133
§ 3. La implementación de la vigilancia electrónica en el vigente Código Procesal Penal de la Ciudad Autónoma de Buenos Aires	135
§ 4. La implementación de la vigilancia electrónica como morigeración de la prisión preventiva en el nuevo Código Procesal Penal Federal (art. 210, inc. "i" de la ley 27.063, t.o. decr. 118/19)	139

## CAPÍTULO VI

**NUEVAS FORMAS DE VIGILANCIA ELECTRÓNICA  
PROPUESTAS EN LOS PROYECTOS DE LEY**

§ 1. Vigilancia acústica .....	145
§ 2. Vigilancia de las comunicaciones electrónicas .....	151
§ 3. Vigilancia remota sobre equipos informáticos .....	166
§ 4. Vigilancia a través de dispositivos de captación de imágenes .....	175
§ 5. Vigilancia a través de dispositivos de seguimiento y de localización .....	182

## CAPÍTULO VII

**DEBIDO PROCESO, VIGILANCIA ELECTRÓNICA  
Y PRUEBA DIGITAL**

-----	196
-------	-----

## CAPÍTULO VII

**VIGILANCIA ELECTRÓNICA E INTELIGENCIA  
ARTIFICIAL**

§ 1. La inteligencia artificial .....	213
§ 2. La inteligencia artificial y el servicio de administración de justicia .....	219
a) Cold Case .....	219
b) Sweetie .....	220
c) VALCRI —Visual Analytics for Sense making in Criminal Intelligence analysis— .....	220
d) CompStat .....	221
e) PredPol .....	221
f) NDAS —National Data Analytics Solution— .....	221
g) Veripol .....	222
h) iBorderCtrl .....	222
i) COMPAS .....	223
1. La escala de riesgo de liberación preventiva .....	223
2. La escala de reincidencia general .....	223
3. La escala de reincidencia en forma violenta .....	223
j) Prometea .....	226
k) Sense Time .....	229
§ 3. La inteligencia artificial y la vigilancia electrónica .....	232

## CAPÍTULO IX

**CONCLUSIONES**

-----	241
-------	-----

**ANEXOS**

ANEXO I

**COMPENDIO NORMATIVO**

I. Resolución MJyDH 808/16 .....	251
II. Resolución MJySGC 484/16 .....	254
III. Resolución SSJUS 285/16 .....	260

ANEXO II

**CONVENIO SOBRE LA CIBERDELINCUENCIA**

.....	275
-------	-----

ANEXO III

**DECLARACIÓN CONJUNTA SOBRE LA COOPERACIÓN ARGENTINO-ESTADOUNIDENSE SOBRE POLÍTICA CIBERNÉTICA**

.....	299
-------	-----

ANEXO IV

**PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO SOBRE LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS ELECTRÓNICAS A EFECTOS DE ENJUICIAMIENTO PENAL {SWD(2018) 118 FINAL} - {SWD(2018) 119 FINAL}**

A. Exposición de motivos .....	301
B. Reglamento .....	329
C. Anexos de la propuesta de reglamento .....	364

ANEXO V

**INSTRUMENTOS Y DOCUMENTOS INTERNACIONALES. ACORDADAS Y RESOLUCIONES**

1. Instrumentos internacionales .....	375
2. Documentos internacionales .....	375
3. Acordadas y resoluciones .....	376
a) Acordadas de la Corte Suprema de Justicia de la Nación .....	376
b) Resoluciones de la Corte Suprema de Justicia de la Nación .....	377
c) Resoluciones MJyDH; MJySGC; SSJUS, MPF, MPD .....	377
d) Normativa de la CABA .....	378

ANEXO VI

**RESEÑA JURISPRUDENCIAL**

1. Jurisprudencia nacional .....	381
2. Jurisprudencia internacional .....	381

<b>BIBLIOGRAFÍA GENERAL</b> .....	383
-----------------------------------	-----