



DANIELA S. DUPUY
Dirección

CATALINA F. NEME
Coordinación

ESTAFAS. DEFRAUDACIONES INFORMÁTICAS.
TÉCNICAS Y MODALIDADES DE CIBERFRAUDE. INVESTIGACIÓN DE CRIPTOACTIVOS:
ENFOQUE TÉCNICO Y JURÍDICO. INCAUTACIÓN Y DECOMISO DE CRIPTOACTIVOS.
INVESTIGACIÓN PASO A PASO. SELECCIÓN DE JURISPRUDENCIA Y LEGISLACIÓN

Prólogo

JAIME CAMPANER (ESPAÑA)

Autores

CRISTIAN BORGHELLO - MARÍA SOL CINOSI

JUAN MANUEL SARRABAYROUSE - NICOLÁS RAMÍREZ

EDUARDO J. RIGGI - FERNANDO RIVAROLA

AGOSTINA MIQUELARENA - FRANCO PILNIK

JAVIER VELLIDO - CRISTIAN FARIÑA - JUAN MANUEL MADARIAGA

Entrevistas

HORACIO AZZOLIN - MATÍAS FERNÁNDEZ NOGUERA



CONTENIDO AUDIOVISUAL

h
hammurabi
JOSE LUIS DEPALMA EDITOR

ÍNDICE GENERAL

NÓMINA DE AUTORES Y ENTREVISTADOS	9
PRÓLOGO	23
PRESENTACIÓN	27
ABREVIATURAS	31

PRIMERA PARTE

DOGMÁTICA Y MODALIDADES DE CIBERFRAUDES

1.

LOS CIBERFRAUDES DENTRO DE LA TEORÍA GENERAL DE LAS DEFRAUDACIONES

NICOLÁS RAMÍREZ

§ 1. Consideraciones generales. Bien jurídico	35
a) Bien jurídico protegido. Patrimonio	35
b) Defraudaciones por engaño y por abuso de confianza	37
§ 2. Los elementos de la estafa. Su relación con los ciberfraudes	43
a) Ardid o engaño	44
b) Error	46
c) Disposición patrimonial	47
d) Perjuicio patrimonial. La estafa en triángulo	48
§ 3. Conclusión	49

2.

EL DELITO DE ESTAFAS INFORMÁTICAS

¿ESTAFAS INFORMÁTICAS FRENTE A FRAUDES BASADOS EN LA INGENIERÍA SOCIAL O SIMPLEMENTE ESTAFAS?

EDUARDO J. RIGGI

3.

**ANATOMÍA CRIMINOLÓGICA
DEL CIBERDELITO PATRIMONIAL: TÉCNICAS
Y MODALIDADES DEL CIBERFRAUDE**

JUAN MANUEL SARRABAYROUSE

§ 1. El ecosistema del ciberdelito patrimonial	65
§ 2. El ciberdelincuente, la cibervíctima y el ciberdelito	72
a) El ciberdelincuente	72
b) La cibervíctima	75
1. El Estado como cibervíctima	75
2. Las organizaciones como cibervíctimas	76
3. El individuo como cibervíctima	79
§ 3. El ciberdelito patrimonial: técnicas y modalidades del ciberfraude	83
a) Las técnicas empleadas para el ciberfraude: la ingeniería social	83
1. La investigación de fuentes abiertas (OSInt/SocMInt)	84
2. El «phishing» y sus modalidades: «smishing», «vishing» y «spear phishing»	85
3. La técnica de «SIM swap»	90
b) Modalidades delictivas en el ciberfraude	94
1. Ciberfraude bancario	94
2. Ciberfraude de WhatsApp	98
3. Ciberfraude por troyano bancario	103
§ 4. Palabras finales	106

SEGUNDA PARTE

CRIPTOACTIVOS Y BLOCKCHAIN

1.

**EL DELITO DE ESTAFA Y SU RELACIÓN
CON LOS ACTIVOS VIRTUALES**

INVESTIGACIÓN, INCAUTACIÓN Y DECOMISO DE CRIPTOACTIVOS

MARÍA SOL CINOSI

§ 1. Introducción	111
§ 2. Naturaleza jurídica y regulación de los activos virtuales	112
a) Legislación de carácter internacional	112
b) Legislación en América Latina	114
1. Regulación en la Argentina	114
2. Regulación en Brasil	116
c) La Unión Europea	116
d) Estados Unidos de Norteamérica	117
e) Conclusión	118

§ 3. El delito de fraude y su relación con los activos virtuales	118
a) AVs y el «ardid o engaño». EE.UU. Esquema piramidal: OneCoin Ltd.	121
b) AVs y el «objeto material del delito» de estafa. EE.UU. Rug Pulls	122
c) AVs y el delito de fraude, en España	123
d) AVs y el objeto material del delito de estafa. La Argentina	124
e) El fraude y la utilización de AVs para diversificar y ocultar los fondos	126
f) AVs y el delito de lavado de activos. El caso «Bobinas blancas»	132
g) Conclusión	134
§ 4. Dificultades a la hora de investigar	134
a) Billeteras no alojadas	134
b) Mezcladores	135
c) Salto de cadenas	136
d) Fraccionamiento	137
e) Monedas privadas	137
f) Conclusión	138
§ 5. Investigación penal: el análisis de la cadena de bloques	138
a) Trazabilidad mediante el análisis de la cadena de bloques	139
b) Utilización de la cadena de bloques	141
c) Utilización de un explorador público	141
d) Utilización de un explorador privado	142
e) Conclusión	143
§ 6. Investigación en fuentes abiertas	143
§ 7. Etiquetado	144
§ 8. Agrupamiento	145
a) Gasto conjunto	147
b) Pago redondo	147
c) Gasto simple	148
d) Tipo de dirección	148
§ 9. Solicitar información a PSAVs	149
a) Pedido de información a un PSAVs	149
b) PSAVs radicado en el exterior	152
c) El pedido de información «per se»	153
§ 10. Desafíos procesales	154
a) Libertad probatoria	155
b) El análisis de la cadena de bloques y los exploradores privados	156
c) La solicitud de información a un PSAVs	157
d) Jurisprudencia	158
e) Conclusión	160
§ 11. Incautación de activos virtuales	161
a) Billetera alojada	164
b) El PSAVs no colabora / billetera no alojada	165
1. Preparación previa al secuestro de activos virtuales	166
I. Solicitud de orden judicial	166
II. Creación de la billetera controlada por el MPF	167
III. Preparación del personal interviniente	169

2. La incautación de activos virtuales «per se»	169
I. Recreación de la billetera y posterior transferencia	169
II. Transferencia directa	170
III. Copia «bit» a «bit»	171
IV. Consideraciones adicionales	171
V. Consideraciones acerca del procedimiento	173
3. Luego de la transferencia	179
§ 12. Conclusión	181

2.

INTRODUCCIÓN EN LA INVESTIGACIÓN DE CRIPTOACTIVOS

ENFOQUE TÉCNICO Y JURÍDICO

CRISTIAN BORGHELLO

§ 1. Introducción	183
§ 2. La Blockchain y los criptoactivos	186
— Tipos de Blockchains	192
§ 3. Las Blockchain, las criptomonedas y el dinero	193
— Volatilidad y criptoactivos «estables»	194
§ 4. Anonimato «versus» pseudoanonimato	195
§ 5. Anonimato «versus» privacidad	196
— Consenso para escribir en la Blockchain	197
— PoW y «hashes»	198
§ 6. Billeteras y direcciones	199
§ 7. Direcciones públicas y privadas	201
— Esquemas multifirmas	207
§ 8. Actores en el mundo de los activos digitales	208
§ 9. Billeteras frías y calientes	211
a) Billetera caliente	211
b) Billetera fría	211
§ 10. Proceso de KYC	213
§ 11. Investigación con criptoactivos	217
§ 12. Herramientas de investigación	218
§ 13. Investigación en las Blockchains	219
a) Métodos pasivos	220
1. OSINT (Open Source INTelligence)	220
2. Análisis, trazabilidad y seguimiento («tracing»)	221
3. Seguimiento de transacciones a través de la Blockchain	221
4. Gráfico de transacciones	225
5. «Clustering»	228
6. Consideraciones importantes en el uso de herramientas	231
b) Métodos activos	233
1. Participación en la Blockchain	233

2. Solicitud de datos a los Exchanges	233
3. ¿Qué implica obtener la colaboración de la entidad?	234
§ 14. Incautación de criptoactivos	236
a) Billetera caliente	236
b) Billetera fría	237
c) Incautación sobre Metamask	243
§ 15. Normativa internacional aplicable	244

TERCERA PARTE

INVESTIGACIÓN

1.

NUEVAS FORMAS O PROCEDIMIENTOS PARA AGILIZAR LA INVESTIGACIÓN EN CIBERFRAUDES

FERNANDO RIVAROLA - AGOSTINA MIQUELARENA

§ 1. Recepción de la denuncia y medidas iniciales	249
a) La denuncia. Formas de inicio	249
— La denuncia	249
I. Formularios de denuncia	252
II. Aplicaciones web	255
III. Correos electrónicos institucionales	256
b) Resguardo de evidencia digital en poder de la víctima	257
1. Dispositivos y credenciales de la víctima	257
I. Autorización del titular del dispositivo	259
II. Productos de la empresa Meta (Facebook, Instagram y WhatsApp)	261
III. Resguardo remoto de evidencia digital. Protocolo de la provincia de Río Negro	267
IV. «Software» espejo. Protocolo de la provincia del Chubut	271
V. Certificación por actuario o funcionario (escribano), o por terceros de confianza	279
§ 2. Cooperación entre distintas jurisdicciones Red 24/7	280
a) Reglas de competencia territorial y equipos de fiscales	280
— Internet. La Red	280
I. Un caso de análisis	281
II. Reglas de competencia territorial	282
b) Equipos de investigación	283
— Fiscales de distintas jurisdicciones	283
— «Softwares» diseñados y aplicados a la investigación penal	286
§ 3. «Modus operandi» de distintas maniobras	287
— «Malware»	287
— Mekotio («malware») + Fraudes informáticos	287
I. Un caso concreto	288
II. Líneas de investigación	294

2.

ESTAFAS INFORMÁTICAS: ENTENDER EL FENÓMENO PARA UNA INVESTIGACIÓN EFICIENTE

CRISTIAN OMAR FARIÑA - JUAN MANUEL MADARIAGA

§ 1. Introducción	297
§ 2. Medidas de investigación	303
a) Declaración de la víctima	303
b) «Malwares» o programas espías en los dispositivos de las víctimas	306
1. Explicación del fenómeno	306
2. Intervención al personal técnico especializado	309
3. Sobre el desarrollo de estas medidas de investigación contamos con la entrevista realizada al especialista Matías Daniel Fernández Noguera	311
c) «Phishing»	311
d) «Pharming»	312
e) Robo y/o Hurto de dispositivos celulares	313
1. Explicación del fenómeno	313
2. Casuística	314
I. En relación a las cuentas de destino de la maniobra investigada	317
II. Medidas de constatación sobre los domicilios residenciales y laborales de los investigados	319
III. Pedidos de inhabilitación para operar y congelamiento de fondos	323
IV. Resultado de los allanamientos	324
V. Situación procesal de los sospechosos	325
f) «SIM SWAP»	330
1. Explicación del fenómeno	330
— ¿Cómo se gestiona ese cambio de SIM?	337
2. Medidas de investigación	339
I. Empresas de telefonía	339
I.1 Registro de llamadas y de uso de datos móviles	341
I.2 Celdas con georreferencia de las mismas	342
II. Bases de datos comerciales	345
II.1 Solicitud ampliatoria a base de datos comerciales	345
II.2 De actividad	346
II.3 De conexión	346
II.4 Del dispositivo utilizado para llevar a cabo las consultas	346
II.5 De registración	347
II.6 De pago	347
II.7 Relevamiento	348
3. Casuística	348
— Línea de uso del sospechoso	365
g) Medidas de investigación sobre cuentas bancarias o billeteras virtuales	365
— Conociendo el ecosistema bancario	366
I. Mercado Electrónico de Pagos	366
II. Claves bancarias y virtuales	367

II.1 CBU (Clave Bancaria Uniforme)	367
II.2 CVU (Clave Virtual Uniforme)	368
III. Cámaras electrónicas de pago de bajo valor	368
IV. ¿Con qué herramientas de investigación contamos para saber de qué banco o entidad es una CBU/CVU?	370
IV.1 Banco Central de la República de Argentina	371
IV.2 Compulsas en fuentes públicas	371
IV.3 Simulación de transferencias	372
IV.4 Consultas a COELSA	373
V. Entidades bancarias y financieras	374
V.1 Información de básica o de registración del titular de cuenta	374
V.2 Información transaccional	375
V.3 Información de contenido y bancaria	375
V.4 ¿Qué información pedir a una entidad bancaria?	377
V.5 Sobre los datos de identidad de las cuentas	382
VI. Empresas prestatarias de telefonía	382
VI.1 En casos de SIM SWAP o de líneas telefónicas sospechosas	382
VI.2 En casos de teléfonos asociados a los perfiles bancarios	387
VII. Cuentas de correo asociadas a los perfiles bancarios	388
VII.1 Análisis de los log's de conexión que surjan de la investigación	388
VII.2 ¿Qué es una IP?	389
VII.3 ¿Cómo luce una IP?	389
VII.4 ¿Qué es una IP nateada?	390
VII.5 ¿Qué es un huso horario? ¿Para qué sirve en la investigación penal?	391
VII.6 ¿Qué es un log o registro de conexión y cómo se compone?	394
VII.7 ¿Qué puedo obtener a raíz del análisis de esa información?	395
VIII. Device ID	397
§ 3. Estrategias para analizar la evidencia producida	399
— Criterios de análisis	399

3.

TÉCNICAS DE INVESTIGACIÓN

FRANCO PILNIK - JAVIER SEBASTIÁN VELLIDO

§ 1. Medidas cautelares de bloqueo de fondos en las cuentas de destino. Restitución de dinero a las víctimas	403
a) Seguimiento de los fondos	403
1. Aproximación	403
2. Pasos a seguir en la ruta del dinero	404
3. En términos generales ¿Qué información podemos requerir a las entidades que operan en el ecosistema financiero?	405
b) ¿Qué pasa con los movimientos bancarios? Secreto bancario o financiero	405
c) Bloqueo de fondos	408
1. Naturaleza jurídica de la medida. ¿Quién la determina?	409

2. Característica de su puesta en práctica	410
d) Restitución de fondos a las víctimas	412
§ 2. Análisis de la información	415
— Allanamiento y secuestro de evidencia física y digital	415
1. Aproximación	415
2. Allanamientos e identificación de evidencia	415
I. Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital	417
II. Medidas durante el allanamiento	418
II.1 «Triage»	418
II.2 Relevamiento digital remoto	419
II.3 Dispositivos protegidos con claves o datos biométricos	421
§ 3. «Modus operandi» de distintas maniobras	422
a) Estafas simples o «cuentos del tío»	422
1. Aproximación	422
2. Casuística	426
3. Calificación legal de la conducta	431
b) «Skimming», fraudes con tarjetas de crédito	432
— Defraudación por el uso indebido de datos de tarjetas bancarias. Formas de apoderamiento	432
I. «Skimming». Clonado. ¿Equiparación a falsificación de moneda? Art. 285 en función del art. 282 del Código Penal	432
II. Defraudación por el uso no autorizado de datos de tarjetas bancarias. Puntos de compromisos tradicionales y uso indebido para pago de servicios	437
§ 4. Conclusión	439

CUARTA PARTE

JURISPRUDENCIA Y LEGISLACIÓN

LAWCEDIC

SUPLEMENTO PROFUNDIZADO DE JURISPRUDENCIA Y LEGISLACIÓN

443

JURISPRUDENCIA

I. CIBERFRAUDES

— Nueva concepción del principio de territorialidad	444
---	-----

II. CRIPTOACTIVOS

1. Concepto de criptomoneda	445
2. Concepto de criptomoneda. Tipicidad de la conducta del «trader» de criptomonedas	446

3. Desbloqueo compulsivo de teléfono celular	446
4. Expectativa de privacidad en la cadena de bloques y en la información que almacena un «exchange»	447
5. Incautación de criptoactivos	448
BIBLIOGRAFÍA GENERAL	451