

**BIBLIOTECA
ENRIQUE LOW MURTRA**

GUSTAVO BALMACEDA HOYOS

Abogado (Universidad de Chile). Diplomado en la Reforma procesal penal (Universidad de Chile)
Doctor en derecho penal (Universidad de Salamanca). Ex Becario MAEC-AECI
Decano Facultad de Ciencias Jurídicas y Sociales (Universidad Iberoamericana de
Ciencias y Tecnología). Profesor contratado de derecho penal (Universidad de Chile).
Consultor del Centro de Estudios de derecho penal (Universidad de Talca)

**EL
DELITO
DE
ESTAFA
INFORMÁTICA**

**LEYER**



ÍNDICE GENERAL

Presentación	17
Introducción	21
Cuadro N° 1: «Ejemplo de phishing».....	22
Cuadro N° 2: Categorías de ilícito.....	32
Cuadro N° 3: Número de denuncias recibidas por año.....	32
Cuadro N° 4: Pérdidas anuales (en millones de dólares americanos).....	32
Cuadro N° 5: Porcentaje de referencia por pérdida económica.....	32
Cuadro N° 6: Método de contacto	33
Cuadro N° 7: Género de los autores	33
Cuadro N° 8: Género de los denunciantes.....	33
Cuadro N° 9: Edad de los denunciantes	33
Cuadro N° 10: Ejemplo de «carta nigeriana»	34

**PRIMERA PARTE
INFORMÁTICA Y DERECHO PENAL**

**CAPÍTULO PRIMERO
APUNTE CRIMINOLÓGICO SOBRE LA DELINCUENCIA INFORMÁTICA**

1. Introducción.....	45
2. Delimitación de la materia de estudio	51
2.1. Conflictos de calificación	51
2.2. Problemas de clasificación.....	56
3. Los sujetos	59
3.1. En torno al autor	59
3.2. Las víctimas.....	61
4. Los hechos	62
4.1. Permanencia y lesividad	62
4.2. Dificultades de averiguación, prueba y «cifra negra»	67
4.3. Naturaleza transfronteriza	69
5. Conclusiones provisionales	70

**CAPÍTULO SEGUNDO
NUEVAS TECNOLOGÍAS Y CRIMINALIDAD TRANSNACIONAL**

Ley penal aplicable en el espacio virtual

1. Nuevas tecnologías y criminalidad transnacional	71
1.1. Aproximación.....	71
1.2. Crítica a los mecanismos de cooperación internacional (especial referencia a la Convención de Budapest sobre el Cibercrimen).....	74
1.2.1. Consideraciones previas.....	74
1.2.2. Objetivos del Convenio	78
1.2.3. Críticas al Convenio	80
1.2.4. Propuesta de «estafa informática» en el Convenio	82
2. Ley penal aplicable	85
3. Conclusiones provisionales	91

**SEGUNDA PARTE
TIPO CLÁSICO DE ESTAFA Y «ESTAFA INFORMATICA»**

**CAPÍTULO TERCERO
PUNTO DE PARTIDA METODOLÓGICO**

1. Delimitación conceptual.....	95
1.1. Introducción.....	95
1.2. Aproximación al concepto de «manipulación informática»	97
1.3. ¿Fraude informático o estafa informática?	102
2. Naturaleza jurídica del delito de «estafa informática».....	103
2.1. Introducción.....	103
2.2. Teorías	106
2.2.1. Postura mayoritaria	106
2.2.2. Postura minoritaria.....	108
2.2.3. Postura excluyente (negativa)	112
3. Conclusiones provisionales	115

**CAPÍTULO CUARTO
TEORÍA GENERAL DEL DELITO DE ESTAFA**

1. Bien jurídico protegido.....	117
1.1. Introducción.....	117

1.1.1. Planteamiento sistemático.....	117
1.1.2. Aproximación a la noción de «patrimonio»	122
1.2. ¿Bien jurídico individual o colectivo?	126
1.3. El patrimonio individual microsocioal como bien jurídico	130
1.3.1. Contenido del patrimonio	134
1.3.2. Concepto jurídico-penal de patrimonio	135
a. Concepción jurídica del patrimonio.....	138
b. Concepción económica del patrimonio.....	140
c. Concepción mixta o jurídico económica del patrimonio	141
d. Concepción personal del patrimonio	145
2. Tipo objetivo.....	149
2.1. Introducción.....	149
2.2. Sujetos	157
2.3. Conducta típica: «engaño bastante para producir un error»	160
2.3.1. Generalidades.....	160
2.3.2. Determinación del engaño jurídico-penalmente relevante	166
a. Teoría objetivo-subjetiva	166
b. Estafa e imputación objetiva	173
b.1. Consideraciones previas	173
b.2. Riesgo permitido.....	184
b.2.1. Deber de actuar y su determinación.	184
b.2.2. Precisiones terminológicas.	192
b.2.3. Riesgo permitido y estafa (informática).....	200
c. Estafa como lesión de un derecho a la verdad	210
2.3.3. El error: ¿elemento autónomo?.....	211
2.4. Resultado típico: «acto de disposición patrimonial perjudicial»	214
2.4.1. El acto de disposición	214
2.4.2. El perjuicio patrimonial	217
a. Introducción	217

b. Excurso: ¿Qué es el peligro jurídico-penal?	224
c. ¿Perjuicio «efectivo» o «en forma de peligro»?	227
d. Aclaraciones terminológicas	236
e. Consecuencias de la admisibilidad de nuestro concepto de «perjuicio en forma de peligro»	237
f. Delimitación y naturaleza jurídica del «perjuicio en forma de peligro»	240
g. Supuestos relevantes en el «perjuicio en forma de peligro»	245
h. Efectos civiles en el «perjuicio en forma de peligro»	247
i. Perjuicio del «poseedor ilícito» y estafa «de prestación ilícita»	249
3. Tipo subjetivo	251
3.1. Dolo	251
3.2. Ánimo de lucro	254
4. Conclusiones provisionales	257

CAPÍTULO QUINTO
REGULACIÓN LEGAL DEL DELITO DE ESTAFA INFORMÁTICA

1. Introducción	263
2. El modelo «exhaustivo» alemán del § 263a StGB	269
2.1. Tipo objetivo	269
2.1.1. Conducta típica: «incorrecta configuración del programa»; «utilización de datos incorrectos o incompletos»; «utilización no autorizada de datos»; y, «cualquier otra forma de influencia no autorizada en el proceso de tratamiento de datos»	269
2.1.2. Resultado típico: «la influencia en el proceso de tratamiento de datos»	278
2.2. Tipo subjetivo: «dolo» y «ánimo de obtención de una ventaja patrimonial antijurídica»	279
3. El modelo de «definición general» del art. 640 ter CP italiano	279
3.1. Tipo objetivo	279

3.1.1. Conducta típica: la «alteración de cualquier modo del funcionamiento de un sistema informático o telemático» o la «intervención sin derecho con cualquier modalidad sobre datos, informaciones o programas»	279
3.1.2. Resultado típico: «resultado irregular del proceso de elaboración de datos que ha sido objeto de una interferencia indebida con daño ajeno»	290
3.2. Tipo subjetivo: «dolo»	291
4. El modelo de «definición general» del art. 248.2 CP español	292
4.1. Tipo objetivo	292
4.1.1. Conducta típica: «manipulación informática o artificio semejante»	294
4.1.2. Resultado típico: «transferencia no consentida de un activo patrimonial»	299
4.2. Tipo subjetivo: «dolo» y «ánimo de lucro»	306
5. «Intervención del hombre» y estafa informática	306
6. Abusos producidos en cajeros automáticos	311
7. Adelantamiento de la punibilidad de la estafa informática	328
7.1. Introducción: el art. 248.3 CP español	328
7.2. Adelantamiento de la punibilidad en el § 263a (III) StGB	334
8. Concursos	337
8.1. Introducción	337
8.2. Problemas más frecuentes	340
9. Conclusiones provisionales	344

CONCLUSIONES

1. Camino para otorgar una respuesta al problema medular	351
2. Soluciones	353
2.1. Interpretación e imputación objetiva de la estafa informática	353
2.2. «Dimensión transnacional» de la estafa informática	356

2.3. Elementos objetivos y subjetivos de la estafa (informática).....	357
3. Reflexión final: una sugerencia para Chile	365
Bibliografía	371