ÍNDICE SISTEMÁTICO

PRESENTACIÓN. 21

SECCIÓN PRIMERA

ASPECTOS SUSTANTIVOS Y CRIMINOLÓGICOS

CAPÍTULO 1. QUO IMUS, ADULESCENS? MENORES, ADOLESCENTES Y JÓVENES FRENTE A LOS RETOS Y PELIGROS DE LOS AVANCES TECNOLÓGICOS. Alfredo Abadías Selma 25

I. HACIA UNA CONTEXTUALIZACIÓN DE LA CUESTIÓN: ERAS, TIEMPOS Y GENERACIONES. 27
II. RETOS Y DESAFÍOS PARA MENORES, ADOLESCENTES Y JÓVENES COMO COLECTIVO VULNERABLE ANTE LOS AVANCES DE LAS NUEVAS Y NO TAN NUEVAS TECNOLOGÍAS 40
III. CONCLUSIONES, REFLEXIONES Y PROPUESTAS 62

CAPÍTULO 2. ALGUNAS CUESTIONES SOBRE CIBERDELINCUENCIA ECONÓMICA. Daniel González Uriel 69

I. INTRODUCCIÓN 71
II. EL CIBERESPACIO COMO ENTORNO CRIMINÓGENO . . . 75
III. PRINCIPALES CIBERDELITOS ECONÓMICOS 79
1. Aspectos generales 79
2. Principales ciberdelitos económicos 81
2.1. Estafas y ciberestafas (arts. 248-251 CP) 82
2.2. Delitos de daños informáticos (arts. 264-264 quater CP). 88

2.3. Delitos contra la propiedad intelectual e industrial (arts. 270-277 CP) 90
2.4. Blanqueo de dinero (arts. 301-304 CP) 93
IV. ALGUNAS DIFICULTADES PROCESALES EN LA DETECCIÓN E INVESTIGACIÓN DE LOS CIBERDELITOS ECONÓMICOS 96

CAPÍTULO 3. ESTAFAS INFORMÁTICAS. Ángel Luis Perrino Pérez 101

I. ELEMENTOS DEL TIPO 103
II. REGULACIÓN ACTUAL 105
III. SUPUESTOS MÁS COMUNES DE ESTAFAS COMETIDAS A TRAVÉS DE LAS TIC 115
IV. LAS «MULAS BANCARIAS» Y SU CALIFICACIÓN JURÍDICA 117
V. CUESTIONES DE COMPETENCIA 122

CAPÍTULO 4. ASPECTOS SUSTANTIVOS Y PROCESALES DE LAS CIBERESTAFAS (PHISHING, SMISHING, VISHING Y PHARMING). Jorge Ibarburen González 125

I. INTRODUCCIÓN 127
II. ORIGEN Y DEFINICIÓN DE LAS CIBERESTAFAS MÁS COMUNES 128
1. Phishing 128
2. Vishing 130
3. Pharming 130
4. Smishing 131
III. ASPECTOS PROCESALES MÁS RELEVANTES 133
1. Competencia objetiva, funcional y territorial de los Juzgados y Tribunales españoles 133
2. Diligencias a practicar en sede de instrucción 135
IV. ASPECTOS SUSTANTIVOS MÁS RELEVANTES DEL DELITO DE ESTAFA INFORMÁTICA 136
1. Evolución histórica 136
2. Elementos configuradores del delito de ciberestafa . . . 139

2.1. Sujeto activo 139
2.1.1. Autor material 140
2.1.2. Cooperador necesario 140
2.1.3. Cómplice 141
2.1.4. Partícipe a título lucrativo 142
2.2. Sujeto pasivo 142
2.3. Penalidad 142
2.4. Elementos del tipo 143
2.4.1. Bien jurídico protegido 143
2.4.2. Engaño previo 143
2.4.3. Error esencial 144
2.4.4. Desplazamiento patrimonial 144
2.4.5. Relación de causalidad entre el engaño y el desplazamiento patrimonial . . 145
2.4.6. Perjuicio 145
2.4.7. Elemento subjetivo del injusto 146
2.5. Actos preparatorios 146
2.6. Grado de ejecución del delito 147
V. CONCLUSIONES 148

CAPÍTULO 5. MODELOS DE INTELIGENCIA ARTIFICIAL QUE OPERAN EN EL CIBERESPACIO: UN NUEVO CAMPO PARA LA CIBERDELINCUENCIA CONTRA LA PROPIEDAD INTELECTUAL. Javier Gómez Lanz 149

I. INTRODUCCIÓN 151
II. TUTELA PENAL DE LOS ALGORITMOS 154
III. ENTRENAMIENTO DE MODELOS DE IA GENERATIVA CON OBRAS PROTEGIDAS POR DERECHOS DE PROPIEDAD INTELECTUAL 159
IV. TUTELA DE LOS PRODUCTOS DERIVADOS DE LA ACTIVIDAD DE LA IA GENERATIVA 166

CAPÍTULO 6. INTELIGENCIA ARTIFICIAL EN LA PREVENCIÓN Y REPRESIÓN DEL BLANQUEO DE DINERO. Prof. Dr. Dr. h. c. mult. Miguel Abel Souto 171

CAPÍTULO 7. RETOS DE LA CIBERDELINCUENCIA PARA LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS: EL PROBLEMA DE LAS SOCIEDADES PANTALLA. Carlos Gómez-Jara Díez. 183

I. INTRODUCCIÓN 185
II. FUNDAMENTOS TEÓRICOS DE LA SOLUCIÓN A PROBLEMAS DE LAS SOCIEDADES PANTALLAS: EL SURGIMIENTO DEL ACTOR CORPORATIVO COMO PERSONA JURÍDICA IMPUTABLE. 186
III. LA RECEPCIÓN EN LA JURISPRUDENCIA DE LA INIMPUTABILIDAD DE LAS SOCIEDADES PANTALLA 195

CAPÍTULO 8. CIBERESPACIO, RESPONSABILIDAD PENAL DE LA MATRIZ POR HECHOS COMETIDOS POR SUS FILIALES Y RESPONSABILIDAD EN EL SENO DE GRUPOS DE EMPRESAS. Alejandro Abascal Junquera 209

I. A MODO DE INTRODUCCIÓN 211
II. LA RESPONSABILIDAD PENAL DE LA MATRIZ POR LOS HECHOS COMETIDOS POR LAS FILIALES 212
III. LA RESPONSABILIDAD PENAL EN EL SENO DE LOS GRUPOS DE EMPRESAS Y LOS PROGRAMAS DE CUMPLIMIENTO NORMATIVO 230

CAPÍTULO 9. DISCURSO DE ODIO EN REDES SOCIALES: NUEVOS RETOS PARA UN VIEJO PROBLEMA. María Teresa Verdugo Moreno. 239

I. INTRODUCCIÓN 241
II. MARCO LEGAL INTERNACIONAL 242
III. EL DISCURSO DE ODIO EN LA LEGISLACIÓN ESPAÑOLA 245
1. Antecedentes. 245

2. Regulación actual 247
IV. CRITERIOS PARA IDENTIFICAR EL DISCURSO DE ODIO PUNIBLE 252
V. EL DISCURSO DE ODIO EN EL CIBERESPACIO. 254
1. Investigación y autoría. 256
2. Penalidad 260
VI. CONCLUSIÓN. 264

CAPÍTULO 10. CIBERDELINCUENCIA, DATOS POLICIALES Y PENITENCIARIOS. DERECHOS DIGITALES DE LAS PERSONAS EN PRISIÓN. Ángel Luís Ortiz González 267

I. EVOLUCIÓN DE LA CIBERCRIMINALIDAD. DATOS POLICIALES 269
II. DATOS PENITENCIARIOS RELACIONADOS CON ESA ACTIVIDAD DELICTIVA Y PROGRAMAS DE TRATAMIENTO QUE SE OFRECEN A LOS CONDENADOS POR ESE TIPO DE DELITOS. 272
III. INTELIGENCIA ARTIFICIAL Y PRISIÓN 283
IV. DERECHOS DIGITALES DE LAS PERSONAS EN PRISIÓN . . 286

SECCIÓN SEGUNDA

ASPECTOS PROCESALES

CAPÍTULO 11. JURISDICCIÓN Y COMPETENCIA PENAL EN EL CIBERESPACIO. Diego Alberto Gutiérrez Azanza 293

I. PLANTEAMIENTO DE LA CUESTIÓN 295
II. EL CIBERESPACIO Y SU NECESIDAD DE REGULACIÓN. . . 296
III. CASOS RELEVANTES CON CONFLICTOS JURISDICCIONALES 300
1. El caso «Megaupload». 300
2. El caso «Yahoo» 302
3. Caso Wintersteiger vs. Products 4U 305
4. Caso Dow Jones & Co Inc. v. Gutnick 307

IV. SOLUCIONES APLICABLES 309
V. ATRIBUCIÓN DE COMPETENCIA TERRITORIAL EN ESPAÑA 316

CAPÍTULO 12. LA INSTRUCCIÓN JUDICIAL DE LOS DELITOS INFORMÁTICOS. DILIGENCIAS DE INVESTIGACIÓN. María Ángeles Velázquez Martín 319

I. INTRODUCCIÓN 321
II. CUESTIONES QUE INFLUYEN EN LA INSTRUCCIÓN. 321
1. Deslocalización. El ciberespacio internacional 321
2. Jurisdicción y competencia 322
3. Diligencias transfronterizas 322
4. Las víctimas. 323
4.1. Víctimas sensibles. 323
4.2. Delitos masa 323
4.3. Delitos multietapa. 323
5. Conocimientos técnicos específicos. Unidades de investigación especializada 323
6. Determinación del autor 324
III. MEDIOS DE COMISIÓN 324
1. Dispositivos electrónicos. 324
2. Internet 324
3. Las redes sociales 324
4. El correo electrónico 325
5. Criptomonedas o criptoactivos 325
IV. COMPROBACIÓN DE LOS HECHOS Y SU AUTOR. DILIGENCIAS DE INSTRUCCIÓN. 325
1. Medidas iniciales. 325
2. Jurisdicción y competencia 326
3. Tipo de procedimiento 326
4. Medidas cautelares 326
5. Secreto de las actuaciones. 327
6. Esclarecimiento de los hechos. 327

7. Denuncia o querella 327
8. Atestado policial 328
9. Declaración del investigado 329
10. Informe pericial 330
V. DILIGENCIAS DE INVESTIGACIÓN ESPECÍFICAS EN DELITOS CIBERNÉTICOS 330
1. Requisitos para la adopción de medidas de intervención tecnológica 331
2. Interceptación de las comunicaciones telefónicas y telemáticas 334
2.1. Datos que pueden obtenerse de la intervención 335
2.2. Medios telemáticos de comunicación objeto de intervención 337
3. Intervención de dispositivos 339
3.1. Datos que podemos obtener 340
4. Registro en remoto de un dispositivo 341
5. Agente encubierto informático 342
VI. CADENA DE CUSTODIA DE LAS EVIDENCIAS 342

CAPÍTULO 13. DOCTRINA JURISPRUDENCIAL SOBRE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA Y SU EFICACIA EN LA LUCHA CONTRA LA E-VIOLENCIA DE GÉNERO. Laura Cristina Morell Aldana 345

I. A MODO DE INTRODUCCIÓN 347
II. LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA 348
1. La interceptación de las comunicaciones telefónicas y telemáticas 349
2. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos 350
3. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización 352
4. Registro de dispositivos de almacenamiento masivo de información 353
5. Registros remotos sobre equipos informáticos 355
III. PRESUPUESTOS COMUNES 356

1. Principios rectores 356
1.1. Principio de especialidad 356
1.2. Principio de idoneidad 357
1.3. Principios de excepcionalidad y necesidad. . . . 357
1.4. Principio de proporcionalidad 359
1.5. Solicitud de autorización judicial: sujetos legitimados y contenido esencial 360
1.6. Resolución judicial que concede la medida . . . 361
1.7. Secreto 364
1.8. Duración y prórroga 364
1.9. Control de la medida 365
1.10. Afectación a terceras personas 366
1.11. Hallazgos casuales 366
1.12. Cese de la medida y destrucción de registros . . 367
IV. E-VIOLENCIA DE GÉNERO. EVIDENCIAS DIGITALES, CUSTODIA DE LA PRUEBA E INCORPORACIÓN DE LA PRUEBA DIGITAL 368
1. E-violencia de género 368
2. Evidencias digitales. Incorporación de la prueba digital en los delitos de e-violencia de género 370
2.1. Las evidencias digitales. 370
2.2. Incorporación de la prueba digital en los delitos de e-violencia de género. 371
2.2.1. Comunicaciones por medio de aplicaciones de mensajería instantánea 373
2.2.2. Grabaciones de conversaciones privadas 375
2.2.3. Correos electrónicos 375
2.2.4. Pantallazos y elementos multimedia . . 377
2.2.5. Agenda del teléfono móvil y número PIN 378
V. CONCLUSIONES 379

CAPÍTULO 14. RETOS POLICIALES EN LA LUCHA CONTRA EL FRAUDE ONLINE. Beatriz Gómez Hermosilla 383

I. INTRODUCCIÓN 385
II. PERFIL DE LOS CIBERESTAFADORES 387
III. DIFICULTADES INVESTIGATIVAS Y PROCESALES 388
IV. HERRAMIENTAS DE INVESTIGACIÓN CON HABILITACIÓN JUDICIAL 391
V. CONCLUSIONES 395

CAPÍTULO 15. COOPERACIÓN JUDICIAL CONTRA LA CIBERDELINCUENCIA. LA PRUEBA DIGITAL INTERNACIONAL. Joaquín Delgado Martín 397

I. NECESIDAD DE LA COOPERACIÓN JUDICIAL INTERNACIONAL FRENTE A LA CIBERDELINCUENCIA. 399
1. Desafíos para la persecución de los ciberdelitos 399
1.1. Volatilidad. Peligro de pérdida de datos 399
1.2. Complejidad técnica. Desafíos de las novedades tecnológicas 400
1.3. Localización de los datos. Internacionalización 401
2. Complejidad de la prueba digital internacional 401
2.1. Falta de un marco legal adecuado 402
2.2. Dificultades en la obtención de datos en poder de los proveedores de servicios. 403
II. PREVENCIÓN Y SOLUCIÓN DE CONFLICTOS DE JURISDICCIÓN EN LA CIBERDELINCUENCIA 404
1. Prevención de conflictos 404
2. Solución de los conflictos de jurisdicción 405
III. LA PRUEBA DIGITAL INTERNACIONAL 407
1. Cooperación judicial Clásica. 407
1.1. Normativa. 407
1.2. Fases de la cooperación judicial internacional . 408
2. El convenio de Budapest 409

2.1. Asistencia mutua para medidas provisionales . . 409
2.2. Asistencia mutua para remisión de datos 411
2.3. Acceso transfronterizo a datos 411
2.4. Otras formas: obtención en tiempo real 412
2.5. Supuestos de urgencia 412
3. Cooperación judicial con Estados Unidos 412
IV. ASISTENCIA JUDICIAL PARA OBTENER PRUEBA DIGITAL EN LA UNIÓN EUROPEA 413
1. Orden Europea de Investigación 413
1.1. Conservación rápida de datos 413
1.2. Remisión de los datos 415
1.2.1. Emisión por órgano español 415
1.2.2. Ejecución en España 417
2. Instrumentos institucionales para mejorar la asistencia judicial en la UE 422
2.1. Instituciones 422
2.2. Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust). 423
2.3. Catálogo de instrumentos web de apoyo a la asistencia judicial 423
3. Colaboración de los prestadores de servicios de intermediación con el sistema penal. Reglamento DSA . . . 424
3.1. Colaboración voluntaria 425
3.2. Obligaciones de colaboración para la persecución de delitos 425
V. PANORAMA DE FUTURO. 426
1. Segundo Protocolo del Convenio de Budapest 426
2. Nuevo sistema en la UE: sistema E-Evidence 428
3. Sobre el Reglamento E-Evidence 430
3.1. Ámbito de aplicación 430
3.1.1. ¿Cuál es el objeto? 430
3.1.2. ¿Qué datos pueden ser objeto de una Orden? 431
3.2. Emisión de la Orden 435

3.2.1. ¿Qué autoridades pueden emitir las órdenes? 435
3.2.2. ¿Cuál es la forma de emisión? 435
3.2.3. ¿Cuál es la forma de remisión? 435
3.3. Ejecución de la Orden 436
3.3.1. Orden de Conservación 436
3.3.2. Orden de Producción 436
VI. EPÍLOGO. RECOMENDACIONES PARA MEJORAR LA OBTENCIÓN INTERNACIONAL DE DATOS 437
1. Estrategia general 437
1.1. Agotar fuentes abiertas y recursos internos 437
1.2. Solicitud internacional alternativa a la Comisión Rogatoria formal 437
1.3. Uso de la Asistencia Judicial Internacional 438
2. Decálogo de recomendaciones para mejorar las solicitudes de cooperación judicial internacional 438
3. Acceso a datos abiertos al público 439
3.1. Identificar propietarios de nombres de dominio 440
3.2. Fuentes abiertas 440
4. Entrega voluntaria por el proveedor de servicios a requerimiento de la autoridad pública 441

CAPÍTULO 16. LOS EQUIPOS CONJUNTOS DE INVESTIGACIÓN PENAL. José Villodre López 443

I. INTRODUCCIÓN 445
II. CONCEPTO 446
III. NORMATIVA 447
IV. CONSTITUCIÓN 449
1. La fase previa: autorización del ministerio de justicia . 449
2. El acuerdo constitutivo, especial referencia al rol de las policías autonómicas y al modelo de liderazgo . . . 452
V. FUNCIONAMIENTO 460
VI. FINALIZACIÓN: EVALUACIÓN DE LOS EQUIPOS CONJUNTOS 462