

ÍNDICE

PRÓLOGO - CARLOS GARCÍA VALDÉS

INTRODUCCIÓN - ESTEBAN MESTRE DELGADO

I. La brusca y no programada obsolescencia de los ordenamientos penal y procesal penal en la España finisecular

II. La irresistible ascensión de la ciberdelincuencia en el mundo contemporáneo

III. La lucha contra la impunidad. La lenta superación de la obsolescencia normativa frente a la ciberdelincuencia

1. Los cambios en la legislación penal material
2. Las reformas de la Ley de Enjuiciamiento Criminal

IV. La cibercriminalidad como concepto penal en construcción

1. El debate conceptual
2. El fundamento de una regulación dispersa
3. Una propuesta de sistematización
 3. 1. Las nuevas tecnologías como medio de comisión del hecho delictivo
 3. 2. La infraestructura informática, electrónica o cibernética como objeto de la agresión (cometida o no a través de medios tecnológicos)
 3. 3. El funcionamiento del sistema informático, electrónico o cibernético como objeto de la agresión
 3. 4. El acceso in consentido a sistemas y servicios informáticos, electrónicos y cibernéticos
 3. 5. Y la apropiación de los datos contenidos en un sistema informático, electrónico o cibernético

V. Los dispositivos informáticos y electrónicos como instrumentos de investigación de actividades delictivas y fuentes de prueba en su enjuiciamiento

1. Tecnología contra tecnología
2. El uso de las nuevas tecnologías en la investigación de los delitos y el conflicto con el derecho a la intimidad
3. Cauces de articulación de la prueba de la comisión de los delitos cibernéticos en el proceso penal español

VI. Es necesario resetear

I. DERECHO PENAL PARTE ESPECIAL

LOS MENORES COMO COLECTIVO VULNERABLE EN LA ERA DE LA “CULTURA TOUCH”

ALFREDO ABADÍAS SELMA

I. Introducción

II. Marco normativo

III. El impacto de la ciberdelincuencia frente a los menores como colectivo vulnerable

IV. La reciente reforma de la normativa de protección del menor

V. Conclusiones y propuestas

VI. Referencias bibliográficas

CYBERSTALKING: ANÁLISIS JURISPRUDENCIAL DEL ART. 172 TER CP. ESPECIAL REFERENCIA A SU COMISIÓN A TRAVÉS DE LAS TIC

SERGIO CÁMARA ARROYO

I. Introducción

II. Concepto y tipificación del cyberstalking

III. Bien jurídico protegido

IV. Sujeto activo y sujeto pasivo

V. Elementos objetivos nucleares: insistencia/reiteración de la conducta y resultado exigido

VI. Elemento subjetivo

VII. Antijuridicidad: el elemento negativo de falta de legitimidad

VIII. Subtipo agravado de violencia de género

IX. Modalidades comisivas. especial referencia al cyberstalking

1. Vigilancia virtual, persecución digital, control y búsqueda de cercanía a través de las redes sociales
2. Establecer o intentar establecer contacto a través de las TIC
3. Suplantación de identidad y ciberacoso: adquirir productos, mercancías, contratar servicios mediante el uso indebido de sus datos personales y hacer que terceras personas se pongan en contacto con la víctima mediante el uso indebido de sus datos personales
4. Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella

X. Bibliografía consultada

LOS DELITOS DE CHILD GROOMING Y DE EMBAUCAMIENTO PARA OBTENCIÓN DE MATERIAL PORNOGRÁFICO: ART. 183 TER CP

FRANCISCO JAVIER BRETONES ALCARAZ

I. Introducción

II. Antecedentes normativos europeos. su transposición al CP español

III. Naturaleza y conducta típica del delito de child grooming

1. Elementos objetivos del tipo
 1. 1. Contacto con el menor de 16 años a través medios tecnológicos
 1. 2. La propuesta de un encuentro
 1. 3. Ejecución de actos materiales encaminados al acercamiento
2. Elementos subjetivos

IV. Error de tipo y error de prohibición

1. Error de tipo
2. Error de prohibición

V. Problemas concursales

VI. Delito de embaucamiento para obtención de material pornográfico

VII. Exclusión de la responsabilidad penal del art. 183 quater CP

PORNOGRAFÍA INFANTIL

EDUARDO DE URBANO CASTRILLO

I. Introducción

II. El derecho penal sexual y los menores

1. Ámbito universal
2. Ámbito europeo

III. Conductas delictivas relativa a la pornografía inf antil

1. Enumeración
2. Examen

IV. El artículo 189 CP, en particular

1. Conductas delictivas
2. Subtipos agravado y atenuado
 2. 1. Establece el Código una serie de supuestos agravados en los que la pena de prisión va de cinco a nueve años si concurre alguna de las circunstancias siguientes
 2. 2. Tipos atenuados

V. Otras cuestiones relacionadas con el delito de pornografía infantil

1. El menor víctima y la valoración de su edad
2. La pluralidad de sujetos pasivos
3. La prueba de la autoría
4. La continuidad delictiva
5. Los concursos delictivos
6. El error

7. La tentativa
8. Atenuantes
9. La responsabilidad de los proveedores de servicios de internet

VI. Bibliografía utilizada

DELINCUENCIA CIBERNÉTICA Y DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

ENRIQUE SANZ DELGADO

I. Introducción

II. Art. 197. 1 CP

III. Art. 197. 2

IV. Art. 197. 3

V. Art. 197. 4

VI. Art. 197. 5

VII. Art. 197. 6

VIII. Art. 197. 7

IX. Art. 197 bis

X. Art. 197 ter

XI. Art. 197 quáter

XII. Art. 197 quinquies

XIII. Art. 198

XIV. Art. 199

XV. Art. 200

XVI. Art. 201

XVII. Bibliografía consultada

INJURIAS ONLINE: LA LESIÓN DEL DERECHO AL HONOR EN LAS REDES SOCIALES

SARA CAROU GARCÍA

I. Introducción

II. La injuria en el ordenamiento jurídico español

III. Libertad de expresión y derecho al honor: la tensión permanente entre instrumentalización de un derecho como medio de comisión del delito y el bien jurídico afectado

1. El derecho al honor

1. 1. La dimensión interna del honor: la propia estimación

1. 2. La proyección exterior del honor: la fama

1. 3. La configuración jurídica del honor: la dignidad de la persona como cobijo del concepto honor

2. La libertad de expresión

IV. La gravedad de la injuria

V. El animus iniuriandi

VI. El espacio virtual de comisión del delito: las redes sociales y la publicidad de la injuria

VII. Aspectos procesales

1. Identificación del querellado

2. El valor probatorio de las capturas de pantalla

3. Necesidad de la existencia de un acto de conciliación

VIII. Conclusiones

IX. Bibliografía

LAS CIBERESTAFAS

ESTEBAN MESTRE DELGADO

I. Introducción

II. Los elementos clásicos del delito de estafa (como marco referencial de las ciberestafas)

1. El tipo básico

1. 1. Una mecánica comisiva basada en la construcción de un engaño

1. 2. Una situación de error en la víctima, causada por el engaño antecedente

1. 3. Un acto de disposición patrimonial, por parte de la víctima, o de un tercero manejado instrumentalmente a ese fin, que se realiza a consecuencia del error inducido

1. 4. Una situación de perjuicio patrimonial en la víctima, resultado final del proceso de engaño y error, y cuya producción efectiva consuma el delito de estafa

1. 5. Y, en la perspectiva subjetiva, un “ánimo de lucro” en el autor del hecho

2. Otras estafas típicas

III. La tipificación expresa de las ciberestafas

1. Las insuficiencias del modelo tradicional del delito de estafa para responder a las defraudaciones a máquinas

2. Un proceso en constante evolución

3. La necesaria próxima reforma del delito de ciberestafa

IV. La acción y el resultado típicos en las ciberestafas

1. La ciberestafa prevista en el artículo 248. 2. a) del Código
2. La modalidad prevista en el artículo 248. 2. b) del Código

V. La individualización de la pena en las ciberestafas

1. Las modalidades agravadas del delito
2. Las formas de ejecución del delito
3. La atribución de responsabilidades penales por la comisión de los delitos de ciberestafa
4. La punición de los delitos de ciberestafa
5. Los concursos
 5. 1. De leyes
 5. 2. De delitos
 5. 3. Delito continuado

EL PHISING Y LA RESPONSABILIDAD PENAL DE LOS MULEROS O CIBERMULAS A LA LUZ DEL ARTÍCULO 248. 2. A) DEL CÓDIGO PENAL

DANIEL FERNÁNDEZ BERMEJO

I. Introducción

II. Análisis de los elementos de la modalidad delictiva del art. 248. 2. a) del Código Penal

III. Los conceptos de manipulación informática y artificio semejante establecidos en el artículo 248. 2. a) del Código Penal

1. Concepto de manipulación informática
2. Concepto de artificio semejante

IV. El phising en el Derecho Penal

V. Tratamiento jurisprudencial de la responsabilidad penal de los muleros o cibermulas y de aquellos que participan en el phising

VI. Breves connotaciones jurisprudenciales sobre las distintas calificaciones de responsabilidad penal de los muleros

1. Autoría
2. Coautoría
3. Cooperación necesaria
4. Imprudencia

VII. Bibliografía

MODALIDADES AGRAVADAS DE ESTAFA MEDIANTE LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

I. Introducción

1. Delimitación de objeto del capítulo
2. Configuración actual de las modalidades agravadas de estafa

II. Ámbito de aplicación de los tipos agravados

III. Consideraciones generales sobre los tipos agravados del artículo 250 CP

1. La importancia de los tipos agravados de estafa en diversos ámbitos
2. Consecuencias dogmáticas de la configuración de los supuestos del art. 250 CP como tipos cualificados de estafa

IV. Examen de los tipos agravados de estafa

1. Cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social
 1. 1. El n.º 1 del art. 250. 1 CP y las estafas informática
 1. 2. Fundamento de la agravación de la pena en el art. 250. 1. 1 CP
 1. 3. Alcance del n.º 1 del art. 250. 1 CP
2. Abuso de firma de otro o sustracción, ocultación o inutilización de expediente, protocolo o documento público u oficial
 2. 1. El n.º 2 del art. 250. 1 CP y las estafas informáticas
 2. 2. Fundamento de la agravación de la pena en el art. 250. 1. 2 CP
 2. 3. Alcance del n.º 2 del art. 250. 1 CP
3. Bienes que integren el patrimonio artístico, histórico, cultural o científico
 3. 1. El n.º 3 del art. 250. 1 CP y las estafas informáticas
 3. 2. Fundamento y alcance del art. 250. 1. 3 CP
4. Especial gravedad en función del perjuicio causado y de la situación económica en que se deje a la víctima o a su familia
 4. 1. El n.º 4 del art. 250. 1 CP y las estafas informáticas
 4. 2. Fundamento de la agravación de la pena en el art. 250. 1. 4 CP
 4. 3. Alcance del n.º 4 del art. 250. 1 CP
5. Estafa por valor superior a 50. 000 euros o por afectar a un elevado número de personas
 5. 1. El n.º 5 del art. 250. 1 CP y las estafas informáticas
 5. 2. El fundamento de la agravación de la pena en el art. 250. 1. 5 CP y el sistema de escalas por el importe de la defraudación
 5. 3. Alcance de las modalidades agravadas del n.º 5 del art. 250. 1 CP
 - A) Problemas de continuidad delictiva con respecto a la modalidad de más de 50. 000 €

- B) La indeterminación de la modalidad relativa a un elevado número de personas y su relación con el delito masa
- 6. Abuso de relaciones personales o aprovechamiento de credibilidad empresarial o profesional
 - 6. 1. El n.º 6 del art. 250. 1 CP y las estafas informáticas
 - 6. 2. Fundamento de la agravación de la pena en el art. 250. 1. 6 CP
 - 6. 3. Alcance del n.º 6 del art. 250. 1 CP
- 7. Estafa procesal
 - 7. 1. El n.º 7 del art. 250. 1 CP y las estafas informáticas
 - 7. 2. Fundamento y alcance de la agravación de la pena en el art. 250. 1. 7 CP
- 8. Multirreincidencia
 - 8. 1. El n.º 8 del art. 250. 1 CP y las estafas informáticas
 - 8. 2. Fundamento y alcance de la agravación de la pena en el art. 250. 1. 8 CP
- 9. Supuestos hiperagravados

V. Bibliografía citada

DAÑOS INFORMÁTICOS

ALICIA GIL GIL

I. Evolución: los problemas del bien jurídico y la ubicación sistemática

II. El objeto material del delito: la distinción entre “daños informáticos” y “daños a un sistema informático”

III. Daños informáticos. El tipo básico

IV. Tipos agravados de daños informáticos

V. Daños a un sistema informático. Obstaculización o interrupción del funcionamiento del sistema. El tipo básico

1. Borrando, dañando, deteriorando, alterando, suprimiendo, o haciendo inaccesibles datos, programas informáticos o documentos electrónicos ajenos
2. Transmitiendo o introduciendo nuevos datos en el sistema
3. Destruyendo, dañando, inutilizando, eliminando o sustituyendo el propio sistema informático, telemático o de almacenamiento de información electrónica en su conjunto

VI. Tipos agravados de daños a un sistema informático

VII. Actos preparatorios. Artículo 264 ter CP

VIII. Responsabilidad de las personas jurídicas

IX. La excusa absolutoria

X. Bibliografía citada

EL BLANQUEO DE CAPITALS A TRAVÉS DE LAS CRIPTOMONEDAS

XESÚS PÉREZ LÓPEZ

I. Introducción general

II. La definición de “moneda virtual” en la versión reformada de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo

III. Usos ilegítimos de las criptomonedas

IV. El uso ilegítimo de criptomonedas en el contexto del blanqueo de capitales y la aplicación del art. 301 CP

V. La “moneda virtual” en el texto en vigor de la Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, tras su reforma de abril de 2021

VI. Bibliografía básica

LAS FALSEDADES DOCUMENTALES COMETIDAS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

GEMA MARTÍNEZ GALINDO

I. La necesidad de reformar los delitos de falsedad documental para adaptarlos a las nuevas tecnologías

II. La existencia de un nuevo bien jurídico: la autenticidad digital

III. Concepto de documento electrónico o digital

IV. Las falsedades informáticas en documentos

1. Las falsedades en documentos clásicos a través de manipulaciones informáticas
2. La alteración de datos contenidos en soportes o sistemas informáticos
3. La falsedad del certificado digital o firma electrónica

V. La falsedad de certificados electrónicos

VI. La falsificación de tarjetas de crédito y débito y cheques de viaje mediante programas informáticos

VII. El tráfico con documento de identidad falso

VIII. Otras falsedades

EL DELITO DE USURPACIÓN DEL ESTADO CIVIL Y SU COMPLEJA APLICACIÓN EN EL ÁMBITO CIBERNÉTICO

SERGIO CÁMARA ARROYO

ALFREDO ABADÍAS SELMA

I. Bien Jurídico protegido

II. Concepto y naturaleza jurídica

III. Sujetos activo y pasivo

IV. Tipo objetivo y modalidades comisivas. Especial referencia a las conductas cometidas a través de las TIC

1. Usurpar de manera continuada
2. Estado civil
3. Usurpación de la identidad de un fallecido
4. Usurpación total o global de la identidad ajena
5. Perjuicio para la víctima
6. Suplantación de identidad digital. Comisión a través de las TIC

V. Tipo subjetivo

VI. Concursos

VII. Conclusiones

VIII. Referencias bibliográficas

CIBERTERRORISMO

ABEL TÉLLEZ AGUILERA

I. De los delitos informáticos a la ciberdelincuencia

II. Sobre el concepto de ciberterrorismo

1. ¿Adiós al elemento organizacional?
2. El elemento personal: ciberterrorismo versus ciberguerra
3. El elemento instrumental
4. El elemento teleológico

III. El ciberterrorismo en el Derecho español

1. El delito de ciberterrorismo en su concepción estricta. El art. 573. 2 CP

1. 1. Tipo objetivo

1. 2. Tipo subjetivo

A) "Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo"

B) "Alterar gravemente la paz pública"

C) "Desestabilizar gravemente el funcionamiento de una organización internacional"

D) “Provocar un estado de terror en la población o en una parte de ella”

1. 3. Culpabilidad y penalidad
1. 4. Formas de aparición del delito
1. 5. Problemas concursales
1. 6. El problema del lugar de la comisión del delito

2. El delito de ciberterrorismo en su concepción amplia
 2. 1. La apología o enaltecimiento del terrorismo (art. 578 CP)
 2. 2. El adoctrinamiento o radicalización activa (art. 577. 2 CP)
 2. 3. El adoctrinamiento o radicalización pasiva (art. 575 CP)

IV. Epílogo: La lucha contra el ciberterrorismo

II. CUESTIONES DE DERECHO PROCESAL

LA INVESTIGACIÓN Y LA FASE DE INSTRUCCIÓN EN LOS PROCEDIMIENTOS POR CIBERDELITOS

GEMA MARTÍNEZ GALINDO

- I. Las peculiaridades en la investigación policial y judicial en el ámbito de la ciberdelincuencia**
- II. Organismos especializados en la persecución del cibercrimen**
- III. Problemas de competencia y jurisdicción**
- IV. Ciberinvestigación policial**
- V. Orden europea de investigación y comisiones rogatorias internacionales**
- VI. Diligencias judiciales de investigación en el ámbito tecnológico**
 1. Diligencia de entrada y registro e incautación de dispositivos informáticos
 2. Diligencias de desprecinto y clonado de dispositivos y evidencias, y volcado de información
 3. Expurgo y garantías del derecho de defensa
- VII. Responsabilidades civiles exigibles en el proceso penal**

LA PRUEBA PERICIAL INFORMÁTICA Y TECNOLÓGICA

GEMA MARTÍNEZ GALINDO

- I. La complejidad de la prueba en el ámbito de la ciberdelincuencia**
- II. Informática forense**
- III. Elaboración y estructura del informe pericial**
 1. Perito que debe llevar a cabo la investigación y procedimiento

2. Objeto del Informe pericial informático
3. Fuentes de información y cadena de custodia
4. Metodología de análisis, valoración y conclusiones

IV. Presentación del informe pericial en el juzgado y valoración judicial

LA INVESTIGACIÓN Y EL REGISTRO DE DISPOSITIVOS ELECTRÓNICOS

MIGUEL MARCOS AYJÓN

I. La investigación electrónica y los derechos fundamentales afectados

II. Disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica

III. El registro de dispositivos electrónicos

1. Dispositivos sobre los que adoptar la medida
2. Los supuestos regulados en la LECrim
 2. 1. Aprehensión de los dispositivos y su acceso cuando son incautados en un registro domiciliario
 2. 2. La aprehensión o incautación de dispositivos fuera del domicilio
3. La autorización judicial como requisito previo para el acceso a dispositivos electrónicos
4. Excepciones al principio de autorización judicial previa
 4. 1. El consentimiento del investigado
 4. 2. Acceso policial directo en supuestos de urgencia
5. Distinción entre el acceso a datos de comunicación y el acceso a datos de la agenda de contactos
6. Volcado de la información contenida en los dispositivos y la cadena de custodia
7. Acceso a los sistemas informáticos externos
8. Deber de colaboración

IV. El registro remoto de equipos informáticos

V. El registro de dispositivos electrónicos en el anteproyecto de LECrim

VI. Conclusiones

VII. Bibliografía

CIBERCRIMINALIDAD E INVESTIGACIÓN POLICIAL. EL AGENTE ENCUBIERTO INFORMÁTICO

SARA CAROU GARCÍA

I. Introducción

II. La cibercriminalidad: Internet como escenario de la actividad delictiva

III. La investigación de los ciberdelitos

IV. El agente encubierto como mecanismo de infiltración policial

1. Concepto
2. El reconocimiento legislativo de la figura del agente encubierto

V. El agente encubierto informático

1. La incorporación del agente encubierto informático al ordenamiento procesal español
2. Los delitos perseguibles por el agente encubierto informático
3. La policía judicial
4. La voluntariedad de la infiltración
5. Afectación de derechos fundamentales
6. La autorización judicial de la infiltración
 6. 1. El contenido de la autorización judicial
 6. 2. Los contactos previos a la autorización judicial
7. El ámbito de actuación del agente encubierto informático: los canales cerrados de comunicación
8. Las facultades del agente encubierto informático: el problema del intercambio de archivos
9. La repercusión penal de la actividad del agente encubierto
 9. 1. El delito provocado y el agente provocador
 9. 2. La responsabilidad penal del agente encubierto

VI. Conclusiones

VII. Bibliografía

DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICAS

GORGONIO MARTÍNEZ ATIENZA

I. Diligencias tecnológicas con y sin autorización judicial

II. Diligencias tecnológicas sin autorización judicial

1. Consecución de lo público
2. Descubrimientos casuales
3. Acceso a datos identificativos
 3. 1. Identificación mediante número IP (art. 588. ter. k LECrim)
 3. 2. Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes (art. 588 ter. l LECrim)

3. 3. Identificación de titulares o terminales o dispositivos de conectividad (art. 588 ter. m LECrim)
4. Interceptación de las comunicaciones telefónicas y telemáticas urgentes
5. Captación de imágenes en lugares o espacios públicos
6. Seguimiento y localización con dispositivos técnicos urgente
7. Registro urgente de dispositivos de almacenamiento masivo de información

III. Diligencias tecnológicas con autorización judicial

1. Interceptación de las comunicaciones telefónicas y telemáticas no urgentes
2. Captación y grabación electrónica de comunicaciones orales
3. Seguimiento y localización con dispositivos técnicos no urgente
4. Registro de dispositivos de almacenamiento masivo de información no urgente
5. Registros remotos sobre equipos informáticos

IV. Anteproyecto de ley de enjuiciamiento criminal de 2020

V. Agente encubierto informático

VI. Orden de conservación de datos

LA FASE INTERMEDIA EN EL PROCESO PENAL Y LOS DELITOS INFORMÁTICOS

DIEGO JESÚS ROMERO JAIME

I. Introducción

II. La fase intermedia del procedimiento abreviado: desde el auto de transformación hasta el escrito de acusación o de petición de sobreseimiento

1. El auto de transformación en procedimiento abreviado: delimitación subjetiva y objetiva del objeto del proceso penal
2. El escrito de acusación
3. La petición de sobreseimiento
 3. 1. Sobreseimiento provisional
 3. 2. Sobreseimiento provisional total y parcial
 3. 3. Sobreseimiento libre, total o parcial
 3. 4. La resolución sobre la petición de sobreseimiento
4. La solicitud de diligencias complementarias

III. La fase intermedia del procedimiento abreviado: desde el auto de apertura del juicio oral hasta el escrito de defensa

1. El auto de apertura del juicio oral
2. La comparecencia del encausado
3. El escrito de defensa

IV. La conformidad en la fase intermedia del procedimiento abreviado

1. Las modalidades del artículo 784. 3
2. El control de legalidad de la conformidad

V. La fase intermedia en los juicios rápidos

1. Delitos informáticos y juicios rápidos
2. La fase intermedia en los juicios rápidos
3. La conformidad en los juicios rápidos

VI. Bibliografía consultada

EPÍLOGO