ÍNDICE

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

SERGIO CÁMARA ARROYO

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

FRANCISCO JAVIER BRETONES ALCARAZ

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

LAS CIBERESTAFAS

ESTEBAN MESTRE DELGADO

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

LUIS ROCA DE AGAPITO

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.° 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.° 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.° 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.° 2 del art. 250. 1 CP
3. Bienes que integren el patrimonio artístico, histórico, cultural o científico
    3. 1. El n.° 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.° 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.° 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.° 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.° 5 del art. 250. 1 CP
        A) Problemas de continuidad delictiva con respecto a la modalidad de más de 50. 000 €

DAÑOS INFORMÁTICOS

ALICIA GIL GIL

EL BLANQUEO DE CAPITALES A TRAVÉS DE LAS CRIPTOMONEDAS

XESÚS PÉREZ LÓPEZ

LAS FALSEDADES DOCUMENTALES COMETIDAS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

GEMA MARTÍNEZ GALINDO

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)

LA FASE INTERMEDIA EN EL PROCESO PENAL Y LOS DELITOS INFORMÁTICOS

DIEGO JESÚS ROMERO JAIME