ÍNDICE

PRIMERA PARTE - ESTAFA Y CIBERDELITOS

1. MARCO CONCEPTUAL Y DOGMÁTICO DE LA ESTAFA INFORMÁTICA

    1.1. Concepto de estafa tradicional y evolución hacia su modalidad digital

    1.2. Elementos típicos del tipo penal (art. 248.2 a) CP)

    1.3. El “engaño bastante” en el entorno digital

    1.4. El “artificio semejante” y su interpretación jurisprudencial a la luz de la reciente jurisprudencia del TS

    1.5. Diferenciación entre estafa informática y otros delitos cibernéticos afines

2. MODALIDADES COMISIVAS DE LA ESTAFA DIGITAL

    2.1. Phishing, vishing y smishing como fraudes de ingeniería social

        2.1.1 El phishing

            2.1.1.1 El phishing: preguntas clave

        2.1.2 El vishing

            2.1.2.1 Vishing: preguntas clave

        2.1.3 El smishing

            2.1.3.1 El smishing: preguntas clave

    2.2. Pharming, spoofing y malware financiero

        2.2.1 Pharming

            2.2.1.1 Pharming: preguntas clave

        2.2.2 El Spoofing

            2.2.2.1 El Spoofing: preguntas clave

        2.2.3 El Malware financiero

            2.2.3.1 El Malware financiero: preguntas clave

    2.3. Deepfakes y suplantación de identidad digital en contratos

        2.3.1 Dilemas normativos y propuestas de lege ferenda

    2.4. Fraudes por manipulación informática directa (hacking, cracking, skimming)

    2.5. El rol de los “money mules” en redes organizadas de fraude

3. EL BIEN JURÍDICO PROTEGIDO Y LA TUTELA PENAL

    3.1. Patrimonio versus seguridad informática: debate doctrinal

    3.2. Protección de la confianza en los sistemas telemáticos de transacción

    3.3. Estafas en servicios bancarios y financieros digitales

    3.4. Perspectiva de género y grupos vulnerables ante fraudes digitales

    3.5. Criterios para la determinación del perjuicio patrimonial

4. CUESTIONES JURÍDICO-PENALES Y VACÍOS NORMATIVOS

4.1. Lagunas de tipicidad en contextos tecnológicos emergentes

4.2. Desafíos probatorios: prueba electrónica y cadena de custodia

4.3. Internacionalización del delito y competencia jurisdiccional

4.4. Responsabilidad penal de personas jurídicas y “compliance”

4.4.1 Complementos dogmáticos y jurisprudenciales: hacia una responsabilidad penal efectiva

4.5. Ineficacia de los tipos tradicionales frente al “cybercrime-as-a-service”

5. APROXIMACIÓN A LA JURISPRUDENCIA SOBRE CIBERCRIMEN

5.1. STS 838/2023 y el alcance del concepto “artificio semejante”

5.2. Jurisprudencia europea sobre estafa informática (TEDH, TJUE)

5.2.1 El Tribunal Europeo de Derechos Humanos y la estafa informática

5.2.2 El Tribunal de Justicia de la Unión Europea y la estafa digital

5.2.3 Armonización y desafíos pendientes

5.3. La responsabilidad de las entidades bancarias ante el phishing y fraude bancario a la luz de la STS 571/2025 de 9 de abril

5.3.1 Calificación jurídica: estafa informática vs. estafa tradicional

5.3.2 Elementos del tipo: el “engaño bastante” y el desplazamiento patrimonial

5.3.3 Participación y cooperación necesaria

5.3.4 Prueba digital y verificación de los hechos

5.3.5 Necesidad de un tipo penal específico

5.4. Comentario crítico a sentencias representativas

5.4.1 STS 838/2023: La interpretación extensiva del “artificio semejante”

5.4.2 SAP Valencia (Sección 5ª), 3 de julio de 2020: Phishing y engaño suficiente

5.4.3 SAN 246/2019: Responsabilidad penal de la persona jurídica

5.4.4 SAP Madrid, Sección 15ª, 23 de septiembre de 2019: Uso de tarjetas duplicadas

5.4.5 SAP Barcelona, Sección 7ª, 14 de febrero de 2021: Testaferros y responsabilidad por blanqueo

5.5. Impacto de las reformas de la LO 14/2022 en la tipificación penal

5.5.1 Modificación del artículo 248.2 CP: precisión conceptual

5.5.2 Otras modificaciones penales relevantes

5.5.3 Críticas doctrinales: oportunidad perdida

5.5.4 Compliance penal y LO 14/2022

5.5.5 Hacia una futura reforma estructural

6. PREVENCIÓN, DETECCIÓN Y REACCIÓN DEL DERECHO PENAL

- 6.1. Medidas legislativas en el marco de la UE y el Consejo de Europa
- 6.2. Protocolo de investigación penal en delitos informáticos
- 6.3. Políticas públicas y cooperación internacional contra el ciberfraude
- 6.4. La ética judicial en el enjuiciamiento de delitos tecnológicos
- 6.5. Propuestas de reforma y adaptación tecnológica

SEGUNDA PARTE - INTELIGENCIA ARTIFICIAL Y DERECHO PENAL

1. FUNDAMENTOS FILOSÓFICO-JURÍDICOS: LA DOGMÁTICA PENAL ANTE LA IA

- 1.1. Ontología de la IA y categorías penales tradicionales
- 1.2. La noción de acción y el principio de culpabilidad en sistemas automatizados
- 1.3. Imputación objetiva y creación de riesgos artificiales
- 1.4. ¿Es posible la culpabilidad sin conciencia humana? Crítica a las construcciones expansivas

2. LA AUTORÍA Y PARTICIPACIÓN EN DELITOS MEDIADOS POR SISTEMAS INTELIGENTES

3. RESPONSABILIDAD PENAL POR DISEÑO Y ENTRENAMIENTO DE SISTEMAS DE IA

4. EL DELITO COMETIDO POR LA IA: ¿FICCIÓN NORMATIVA O REALIDAD FUTURA?

5. INTELIGENCIA ARTIFICIAL Y DERECHO PENAL PROCESAL

- 5.1 Retos del Derecho Procesal Penal ante la Inteligencia Artificial

6. DERECHO PENAL Y POLÍTICA CRIMINAL EN LA ERA DE LA IA

7. PROPUESTAS DE LEGE FERENDA

8. BIBLIOGRAFÍA