III

2024 N.º 144

cuadernos de política criminal

segunda época

Dykinson, S.L.

III

2024 N.º 144

cuadernos de política criminal

segunda época

Edita

Dykinson, S.L.

AVISO IMPORTANTE A NUESTROS SUSCRIPTORES

Si desea suscribirse a **Cuadernos de Política Criminal**, llame por teléfono o envíe un e-mail a info@dykinson.com, indicando la forma de pago y el número o números a los que quiere suscribirse, e inmediatamente recibirá su pedido.

CPC se adhiere a las Core Practices del Committee on Publication Ethics (COPE) disponibles en: *https://publicationethics.org/core-practices*; y especialmente a los *Principios de Buenas Prácticas y Transparencia en las Publicaciones Académicas* desarrollados por el Committee on Publication Ethics (COPE), Open Access Scholarly Publishers Association (OASPA), Directory of Open Access Journals (DOAJ) y World Association of Medical Editors (WAME) disponibles en: *https://publicationethics.org/ resources/guidelines-new/principles-transparency-and-best-practice-scholarly-publishing*. La Declaración de ética y malas prácticas completa de CPC puede ser consultada en sus versiones en español e inglés: *https://www.dykinson.com/revistas/cuadernos-de-politica-criminal/*

La Revista no se responsabiliza de las opiniones contenidas en los artículos

Edita: Dykinson, S.L.
C/ Meléndez Valdés, 61 — 28015 Madrid
Tels. 91 544 28 46 / 91 544 28 69
Fax 91 544 60 40
info@dykinson.com / www.dykinson.com

Imprime: Safekat, S. L.
Laguna del Marquesado, 32 - 28021 Madrid
www.safekat.com

ISSN: 0210-4059
Depósito Legal: M. 7533-1977
DOI: https://doi.org/10.14679/3796

CONTENIDO

SECCIÓN DE ESTUDIOS PENALES

LA RETROACTIVIDAD DE LA LEY PENAL: LA UTILIDAD DE LAS DISPOSICIONES TRANSITORIAS. *Por Elena Marín de Espinosa* 5

LA LIMITADA PERSEGUIBILIDAD DE LOS DELITOS SOCIETARIOS. *Por Miguel Bustos Rubio* 35

LA NECESIDAD DE TRATAMIENTO EN EL INTERNAMIENTO PSIQUIÁTRICO PENAL: HACIA LA SUPERACIÓN DE LOS MODELOS PENITENCIARIOS. *Por Angelo Giraldi*..... 83

SECCIÓN ESTUDIOS CRIMINOLÓGICOS

EL CONSEJO SOCIAL PENITENCIARIO. *Por Borja Mapelli Caffarena*..... 117

SECCIÓN JURISPRUDENCIAL

PANORAMA JURISPRUDENCIAL: TRIBUNAL CONSTITUCIONAL Y TRIBUNAL SUPREMO. *Por Manuel Jaén Vallejo* 137

SECCIÓN BIBLIOGRÁFICA

RECENSIÓN A LA OBRA «DERECHO PENAL *TRENDING TOPIC*. UNA SEMANA DE COMUNICACIÓN SOBRE LA LEY Y LA JUSTICIA PENAL EN LA RED SOCIAL X (ANTES LLAMADA TWITTER)», FERNANDO MIRÓ LLINARES/ JESÚS C. AGUERRI (EDS.) MARCIAL PONS, MADRID, 2024, 227 PÁGINAS. *Por Roberto Cruz Palmera*..... 151

RECENSIÓN AL LIBRO «APROXIMACIÓN A LA TEORÍA GENERAL DEL DELITO», ANTONIA MONGE FERNÁNDEZ, TECNOS, MADRID, 2024, 268 PÁGINAS. *Por Javier Parrilla Vergara* 157

RECENSIÓN A LA OBRA "PROFILI PENALI DELLA SICUREZZA SUI LUOGHI DI LAVORO, "RISCHI" DI RISPONSABILITÀ OGGETIVA E RIMPROVERO PERSONALE" DE ANGELO GIRALDI, ARACNE, 2024, 332 PÁGINAS. *Por Rosa García Campuzano* 165

RECENSIÓN A LA OBRA "LAS CIBERESTAFAS: TENDENCIAS, INFRACTORES, VÍCTIMAS Y PREVENCIÓN", KEMP, S, ATELIER, BARCELONA, 2024, 189 PÁGINAS. *Por Patricia Saldaña Taboada* 175

NOTA NECROLÓGICA

IN MEMORIA FERRANDO MANTOVANI. *Por Ignacio F. Benítez Ortúzar* 189

IN MEMORIAM CARLOS ROMEO CASANOVA. Por *Lorenzo Morillas Cueva* 195

NOTICIARIO 201

POLÍTICA EDITORIAL, CRITERIOS Y RÉGIMEN PARA LA PUBLICACIÓN DE TRABAJOS ORIGINALES EN CPC 231

RECENSIÓN A LA OBRA "LAS CIBERESTAFAS: TENDENCIAS, INFRACTORES, VÍCTIMAS Y PREVENCIÓN", KEMP, S, ATELIER, BARCELONA, 2024, 189 PÁGINAS

PATRICIA SALDAÑA TABOADA
Departamento de Derecho Penal Universidad de Granada

Es un placer para mí realizar la reseña de la obra del Prof. Steven Kemp, Profesor Lector en Criminología en la Universitat de Girona, quien se ha consolidado como un referente en el estudio del cibercrimen económico. Su dedicada trayectoria investigadora, centrada en las tendencias, la victimización y la prevención del cibercrimen, lo posiciona como una figura relevante en la materia. Los resultados de sus investigaciones han sido publicados en revistas internacionales de prestigio, lo que refuerza la calidad y el rigor de esta obra. Su análisis integral de las ciberestafas, abordando tanto a los infractores como a las víctimas, junto con las estrategias de prevención y las respuestas institucionales, convierte este trabajo en una contribución fundamental al estudio del fenómeno.

El prólogo de la obra ha sido elaborado por el profesor Fernando Miró Llinares, Catedrático de Derecho Penal y Criminología en la Universidad Miguel Hernández de Elche y Director del Centro Crímina para el Estudio y Prevención de la Delincuencia. En este, el profesor Miró Llinares destaca la pertinencia y actualidad de la elección de la ciberestafa como tema central de la monografía, considerando la constante evolución de este fenómeno delictivo y las significativas repercusiones que tiene para la sociedad en términos económicos, sociales y jurídicos. Asimismo, subraya las notables cualidades investigadoras del Prof. Steven Kemp, haciendo énfasis en la rigurosidad que caracteriza su trabajo. Señala, además, el acierto de haber producido una monografía de carácter exhaustivo y completo sobre una temática tan relevante, ofreciendo una herramienta imprescindible para académicos, juristas y profesionales interesados en

el fenómeno de las ciberestafas y su abordaje desde el Derecho Penal y la Criminología.

La obra se organiza en tres bloques temáticos diferenciados: autores, víctimas y prevención. Este esquema permite abordar el fenómeno de las ciberestafas desde una perspectiva integral, abarcando tanto a los sujetos que las perpetran como a quienes las sufren, además de las estrategias para combatirlas. En palabras del autor, esta obra supone un recorrido por las cuestiones de mayor interés criminológico relacionadas con las estafas en la era digital.

Previo al inicio del primer bloque, el Prof. Steven Kemp trata una serie de cuestiones introductorias, relativas a las definiciones y tendencias generales que crearán el panorama necesario para tratar las cuestiones clave que se plantean en su obra.

Desde el inicio de la obra, el autor contextualiza que el fenómeno del engaño con fines ilícitos no es algo nuevo, remontándose incluso al siglo III a.C. en Italia, donde un comerciante de cereales intentó obtener beneficios fraudulentos a través de un préstamo, que acordó devolver con intereses cuando entregara el cargamento a su destino. Sin embargo, el comerciante hundió el barco sin mercancía, se quedó el dinero del préstamo y vendió la mercancía para obtener beneficios económicos. Este es uno de los primeros ejemplos documentados de un estafador. Con este ejemplo, el autor quiere ilustrar que aunque actualmente las estafas hayan evolucionado, adaptándose a los cambios sociales y tecnológicos, la utilización del engaño propio de la estafa es algo que ya se podía observar siglos atrás.

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) ha transformado la comisión de delitos. La globalización permite que miembros de diversas nacionalidades participen en una misma organización delictiva, mientras que la industrialización del fraude digital facilita el intento de engañar simultáneamente a millones de personas. Este fenómeno, ha incrementado la rentabilidad de estos delitos, reflejándose en que la mayoría de los ciberdelitos buscan acceder a datos personales o financieros con fines fraudulentos. Sin embargo, esta evolución también complica la investigación policial, ya que Internet fomenta la aparición de oportunidades delictivas, facilita el anonimato y mantiene a las autoridades rezagadas ante la constante adaptación de los criminales.

No obstante, antes de adentrarse en las tendencias del fraude con mayor detalle, el autor plantea la problemática que surge ante la definición de las ciberestafas. En el contexto español, el Código Penal aborda la estafa en sus artículos 248 y 249. Este último, ha sido reformado

recientemente para incorporar lo expuesto en la Directiva 2019/731 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, que incluye modalidades específicas relacionadas con las TIC, como las estafas bancarias mediante transferencias o el uso no autorizado de tarjetas. Esta actualización refleja la conciencia del legislador sobre las tendencias delictivas asociadas a la digitalización.

No obstante, la definición de ciberestafa plantea desafíos debido a la amplitud de conductas que engloba. En la obra se consideran las estafas como "un acto de engaño intencionado que produce un beneficio económico (o la evasión de una pérdida) para el engañador y una pérdida para la víctima". De esta forma, las ciberestafas son un tipo de fraude para el que se emplea el uso de sistemas o redes informáticas y abarcan desde engaños simples hasta sofisticadas estrategias de ingeniería social. Además, puede tratarse de conductas que se intercambian entre conductas *online* y *offline*, siendo de hecho lo habitual. El autor advierte que esta complejidad dificulta el registro adecuado de los casos, especialmente cuando las víctimas son organizaciones o empresas, donde las modalidades de fraude pueden variar significativamente. A nivel práctico, señala que el término puede intercambiarse con conceptos como el ciberfraude, fraude informático o estafa en línea y ese es el criterio que utiliza a lo largo de toda la obra.

De esta forma, el análisis de las ciberestafas en España enfrenta importantes limitaciones debido a la falta de datos oficiales exhaustivos. Aunque los registros del Ministerio del Interior ofrecen un punto de partida, son insuficientes para reflejar la situación real. Los datos sobre ciberestafas en el territorio español, tal y como señala el autor, son limitados en comparación con datos sobre delitos tradicionales, lo que limita la posibilidad de analizar la amenaza que suponen. A pesar de ello, el autor identifica tendencias claras: las ciberestafas han aumentado rápidamente en la última década, representando una proporción cada vez mayor del total de delitos registrados. Además destaca un importante filtrado de casos en el sistema de justicia penal, lo que reduce la visibilidad de muchos incidentes. Las tendencias también varían según el tipo de ciberestafa, influenciadas por cambios en las actividades cotidianas de la población y por la implementación de medidas preventivas. Aun así, el autor subraya que las ciberestafas se han consolidado como uno de los delitos más frecuentes contra los ciudadanos españoles.

Una vez planteadas las cuestiones previas, la obra comienza con el primer bloque, dedicado a los infractores, donde el Prof. Steven Kemp

analiza las técnicas utilizadas por los ciberestafadores, su nivel de organización y las posibles motivaciones que los impulsan a cometer delitos. Este apartado no solo permite comprender las tácticas y *modus operandi* de los delincuentes, sino que también arroja luz sobre la evolución de su actividad en un entorno digital cada vez más complejo.

Con el objetivo de comprender mejor el *modus operandi* de estos delitos, el capítulo comienza con un análisis a través de un "crime script" para las ciberestafas y *phishing*. Este enfoque descompone el proceso del delito en tres etapas principales: etapa de preparación, etapa de actividad principal y etapa de cobro, huida y encubrimiento. Durante la primera etapa, los estafadores identifican sus objetivos, seleccionan coautores, herramientas y técnicas. El autor subraya la importancia de los espacios en línea, donde los criminales se reúnen para intercambiar ideas, aprender, compartir datos y adquirir servicios esenciales. En la segunda fase, los estafadores interactúan con sus objetivos, a menudo utilizando técnicas de ingeniería social para engañarlos y comenzar a extraer dinero. Esta etapa representa el núcleo de la interacción entre el delincuente y la víctima. Finalmente, en la etapa de cobro huida y encubrimiento se busca maximizar las ganancias mientras se eluden las investigaciones policiales. En este punto, el autor resalta que las "mulas" desempeñan un papel clave en el movimiento de los fondos, aunque se encuentran en el nivel más bajo de la jerarquía organizativa de las redes de ciberestafa.

Debido a la diversidad de conductas que engloba el fenómeno de las ciberestafas, el autor destaca la heterogeneidad en los perfiles de los delincuentes y en las estructuras organizativas que utilizan.

En cuanto a la organización de los ciberestafadores, en la obra se realiza una distinción entre redes y grupos estructurados. En un extremo, se encuentran las organizaciones tradicionales de delincuencia organizada, que ven en las ciberestafas una fuente adicional de ingresos. En el otro, el autor señala que las investigaciones académicas revelan que la mayoría de los grupos de ciberfraude tienen estructuras dinámicas y flexibles, en contraste con los modelos jerárquicos tradicionales. Estos grupos suelen incluir capas diferenciadas de miembros, como líderes principales, facilitadores profesionales, reclutas y mulas. Además, se destaca la importancia de conexiones tanto *online* como *offline* en la creación de redes de confianza y en la colaboración local y global. Conocer estas dinámicas, según el autor, es de gran relevancia para desarrollar estrategias de prevención efectivas.

En relación con el perfil de los ciberestafadores individuales, el análisis del perfil sociodemográfico plantea grandes desafíos debido a la esca-

sez de datos y a las dificultades inherentes a las investigaciones empíricas en este ámbito. En España, por ejemplo, los datos disponibles se limitan a cifras generales sobre fraude informático, sin acceso a información específica sobre las personas condenadas por ciberestafas.

Pese a estas limitaciones, se expone que, en términos demográficos, los ciberestafadores comparten ciertas similitudes con los delincuentes tradicionales, siendo generalmente hombres jóvenes. No obstante, destaca una mayor representación de mujeres y una edad ligeramente superior en comparación con otros delitos contra la propiedad.

Para profundizar en la comprensión de las motivaciones de los ciberestafadores, el autor recurre a teorías criminológicas como la teoría de la elección racional, el aprendizaje social y las técnicas de neutralización. Estas teorías ayudan a explorar los factores que pueden influir en la decisión de un individuo de cometer una estafa digital. En este sentido, se concluye que las motivaciones predominantes son de carácter financiero, mientras que el aprendizaje social actúa como un catalizador en la carrera delictiva.

El capítulo concluye aportando la idea de que en España y Latinoamérica hay una carencia significativa de estudios sobre ciberestafas, lo que limita el desarrollo de estrategias efectivas de prevención. Se subraya la necesidad urgente de mejorar la comprensión de estos delitos y sus autores para enfrentar un problema que genera millones en pérdidas para ciudadanos, empresas y organizaciones públicas.

El segundo bloque se centra en las víctimas. Dentro de este se encuentra el capítulo tres, dedicado a analizar en profundidad el fenómeno de la victimización en ciberestafas. A lo largo de este capítulo, el autor examina las características de los afectados, tanto a nivel demográfico como de personalidad, incluyendo las actividades que los hacen más propensos a ser blanco de ciberestafas. Asimismo, se dedica especial atención al impacto que esta forma de victimización tiene en los individuos y las organizaciones, no solo desde una perspectiva económica, sino también emocional y operativa.

Se trata de un ámbito sobre el cual existe un mayor número de investigaciones empíricas en comparación con el estudio de los ciberestafadores. No obstante, la gran diversidad de fraudes en línea genera una amplia variedad de perfiles de víctimas, lo que supone un desafío a la hora de identificar patrones de victimización. El autor subraya la importancia de estos estudios para la optimización de recursos preventivos, siempre limitados, con el fin de asignarlos de manera eficaz.

En la obra se examinan los factores que predisponen a algunas personas y organizaciones a un mayor riesgo de sufrir ciberfraudes, recurriendo a características demográficas, actividades cotidianas y estilos de vida de las víctimas, teorías criminológicas y otros rasgos disposicionales más allá del autocontrol. Las organizaciones también son consideradas como víctimas de estafas en línea.

En la primera parte del capítulo, se han examinado estudios relacionados con el perfil de las víctimas en términos de características sociodemográficas, de sus actividades en línea o de sus rasgos de personalidad y el solapamiento de todos ellos. La edad es un factor que genera debate. Aunque se tiende a considerar que las personas de avanzada edad son más vulnerables, existen discrepancias en los estudios. El autor concluye que el análisis de los patrones de victimización debe realizarse en función de tipos específicos de estafas, como las estafas románticas o las relacionadas con criptomonedas, para obtener información útil para su prevención. Al mismo tiempo, se identifican ciertas conductas "arriesgadas" que incrementan la posibilidad de victimización, como interactuar con desconocidos en línea, compartir información sensible, realizar inversiones sin garantías o asociarse con individuos de comportamiento desviado. Estas conductas están relacionadas con la teoría del autocontrol, y su estudio permite establecer las bases de intervenciones preventivas tanto para usuarios individuales como para organizaciones. Además del autocontrol, se mencionan otros factores individuales, como los rasgos de personalidad y estilos de vida, que influyen en la vulnerabilidad frente a las ciberestafas.

Las empresas y entidades también son objeto de ciberfraudes. El análisis de estos casos incluye tanto las pérdidas económicas directas como los efectos más sutiles, como el daño reputacional, que puede provocar la pérdida de confianza de los clientes y, por tanto, graves consecuencias financieras.

El Prof. Steven Kemp concluye esta parte del capítulo advirtiendo de la necesidad de evitar culpabilizar a las víctimas, reiterando que la responsabilidad debe recaer en los infractores y en el sistema encargado de prevenir y perseguir este tipo de delitos.

La segunda parte del capítulo se centra en las repercusiones que la victimización por ciberfraude tiene tanto para individuos como para organizaciones, diferenciando entre el impacto económico y otras consecuencias no financieras.

Las ciberestafas suponen un elevado coste económico para la sociedad. Según se muestra en la obra, el Banco Central Europeo, en 2021 re-

gistró transacciones fraudulentas por un valor aproximado de 1.531 millones de euros. En España, datos del año 2019 posicionan al país como el tercero en volumen de fraude por transacción en la Unión Europea y el séptimo en fraude con tarjeta por cada 1.000 habitantes.

El autor vuelve a criticar la ausencia de datos oficiales detallados por parte de instituciones españolas, como los cuerpos policiales o entidades relacionadas con la ciberseguridad. Esta falta de información rigurosa presenta un obstáculo significativo para la prevención, ya que dificulta conocer la verdadera magnitud del problema. Aunque las pérdidas individuales suelen ser de menor cuantía, su gran frecuencia amplifica el problema. Además, existen costes indirectos asociados a la victimización, como el tiempo invertido en la recopilación de pruebas, la denuncia del delito o la participación en procesos judiciales. El sistema español, que requiere realizar denuncias presencialmente en comisarías, supone un coste adicional tanto para las víctimas como para la sociedad en general.

En el caso de las organizaciones, las consecuencias económicas no se limitan a las pérdidas monetarias directas. Las organizaciones afectadas suelen sufrir daños reputacionales que erosionan la confianza de sus clientes, con graves repercusiones económicas. Esta pérdida de confianza puede afectar también a instituciones públicas, debilitando la percepción de su capacidad para proteger los intereses de los ciudadanos.

Más allá del impacto económico, el Prof. Steven Kemp advierte sobre las consecuencias emocionales y sociales de las estafas digitales. Aunque el perjuicio económico es la consecuencia más evidente, subraya la vulnerabilidad psicológica de las víctimas de ciberfraude. En el caso de las estafas románticas, por ejemplo, las consecuencias emocionales se han comparado con las experimentadas en situaciones de violencia doméstica, destacando sentimientos de vergüenza, negación y aislamiento. La vergüenza y el daño psicológico son emociones negativas que dificultan la recuperación de las víctimas, pero además el autor trata el miedo al delito, considerado como el aumento del temor a sufrir nuevas estafas, generando cambios en sus comportamientos y actividades en línea. De esta forma, la mejora en la comprensión de estos efectos resulta esencial para implementar intervenciones más eficaces que aborden tanto el perjuicio financiero como el bienestar psicológico de las víctimas.

El tercer bloque de la obra aborda la prevención y se divide en dos capítulos. En el primero, que se corresponde con el cuarto capítulo, se analizan las intervenciones diseñadas para reducir la incidencia de las ciberestafas y su impacto, prestando especial atención a las instituciones del sistema penal. El segundo capítulo, que es el quinto capítulo, explora

el papel de otros actores que implementan medidas preventivas enfocadas en aspectos humanos o tecnológicos.

De esta forma, el cuarto capítulo examina la respuesta del sistema penal frente a las ciberestafas, poniendo de manifiesto los desafíos y limitaciones de las instituciones policiales y judiciales en su abordaje.

El Prof. Steven Kemp subraya que la gestión de las denuncias, su correcta tramitación y la recopilación de datos son aspectos clave tanto para entender la magnitud del problema como para desarrollar estrategias preventivas y reactivas eficaces. Se analiza la infradenuncia como una problemática central en el tratamiento de las ciberestafas. A pesar de la creciente prevalencia de este delito, el autor expone que solo entre el 20% y el 25% de los fraudes contra particulares llegan a ser denunciados ante la policía. Esta tendencia, similar en otros países, refleja una cifra negra considerable. Entre las razones que explican esta baja tasa de denuncia, se identifican varios factores: el desconocimiento de la propia victimización, el impacto reducido de la pérdida económica o psicológica percibida, la percepción de la inutilidad de la denuncia, la falta de confianza en la policía o desconocimiento sobre dónde acudir y la reticencia a compartir la actividad en línea con las autoridades.

El autor destaca que los niveles de denuncia varían según el tipo de estafa, lo que sugiere que estos factores influyen de manera diferenciada según la modalidad del fraude. La falta de denuncias impide obtener datos fiables, lo que a su vez dificulta la evaluación de políticas públicas y la asignación de recursos preventivos adecuados. Como señala el autor, "no se puede prevenir ni vigilar eficazmente lo desconocido".

La denuncia por parte de las organizaciones constituye un área aún menos explorada debido a la falta de datos oficiales. Esta escasez puede explicarse, en gran parte, por la baja tasa de denuncias y por la preferencia de las empresas por adoptar medidas privadas de control frente a la ciberdelincuencia. El autor identifica diversas razones por las que las organizaciones eligen no denunciar los fraudes informáticos a las autoridades: desconfianza en la capacidad de la policía para ofrecer una respuesta efectiva, la percepción de que los ataques pueden resolverse internamente, la preocupación por el daño reputacional y la reticencia a compartir información sensible sobre su actividad empresarial.

El modelo actual del sistema penal, predominantemente reactivo, presenta limitaciones importantes en el abordaje de las estafas en línea. En España, las denuncias se reciben en comisarías locales, autonómicas o nacionales, y solo aquellas que se consideran relevantes son remitidas a unidades especializadas. No obstante, esta selección puede verse afec-

tada por la falta de formación específica de los agentes y la ausencia de información adecuada sobre la magnitud del problema.

En el 2012, los fraudes informáticos representaban el 1,2% del total de infracciones reportadas al Ministerio del Interior. En 2021, los fraudes informáticos alcanzaron las 267.011 denuncias, equivalentes al 13,6% del total de delitos conocidos. Este crecimiento exponencial revela que el fraude en línea es una amenaza en auge, aunque aún no constituye una prioridad para las autoridades. Una prueba de ello es la imposibilidad de denunciar fraudes informáticos a través de canales en línea, lo que añade dificultades adicionales para las víctimas.

Por todo ello, se identifican diversos desafíos que obstaculizan la eficacia policial frente a las ciberestafas: la falta de recursos y especialistas dedicados exclusivamente al fraude informático, la complejidad de los casos dada la naturaleza transnacional y anónima de este delito, la limitación del intercambio de información entre cuerpos policiales, las dificultades en la localización de sospechosos y la obtención de pruebas digitales y los desafíos en la gestión de víctimas.

Ante estas dificultades, el autor sugiere líneas de mejora orientadas a fortalecer la capacidad de investigación del sistema penal. Estas incluyen la promoción del conocimiento de casos anteriores, el incremento de la formación policial específica y la mejora del apoyo a las víctimas, aspectos que podrían contribuir a aumentar la confianza y la eficacia de la denuncia.

Frente a las limitaciones del sistema penal para abordar este fenómeno de manera efectiva, se observa una creciente participación de actores privados, como empresas de ciberseguridad, en la prevención y gestión de los fraudes en línea. Aunque estas respuestas complementan la labor policial, también reflejan las limitaciones de las instituciones públicas.

El Prof. Steven Kemp concluye el capítulo exponiendo que la ausencia de un sistema adecuado de denuncias y recopilación de datos impide tener una visión clara sobre la extensión, tendencias y naturaleza del ciberfraude, tanto a nivel individual como organizacional. La falta de recursos, la baja prioridad otorgada a este delito y la complejidad inherente a las ciberestafas han derivado en respuestas del sistema penal generalmente ineficaces. Asimismo, señala que las funciones preventivas del derecho penal son difíciles de aplicar en este contexto, debido a la falta de capacidad para identificar sospechosos, recopilar pruebas y ofrecer apoyo efectivo a las víctimas. Pese a los casos de cooperación transnacional exitosos, el autor insiste en la necesidad de una mejora sustancial en la respuesta de la justicia penal al fraude informático, lo cual requiere

recursos suficientes y una voluntad política firme para afrontar esta amenaza creciente.

El quinto capítulo de la obra está dedicado al estudio de las estrategias y herramientas de prevención de las ciberestafas, abordándolas desde dos perspectivas fundamentales: el factor humano y las respuestas tecnológicas. El autor destaca que, aunque diversas entidades y actores participan en la prevención del ciberfraude, la eficacia de estas medidas sigue siendo limitada en la actualidad.

Aunque se conoce en el ámbito de la investigación del cibercrimen la importancia de las estrategias centradas en el factor humano, estas son menos frecuentes que las que recurren a soluciones tecnológicas. Resulta paradójico, según señala el autor, dado que son los seres humanos quienes caen en el engaño y, a su vez, son ellos quienes pueden detectar y evitar muchas actividades fraudulentas. Las estrategias humanas buscan influir en la capacidad y habilidad de los usuarios para reducir la probabilidad de victimización, detectar los fraudes en curso y mitigar los daños derivados de los ataques.

El capítulo analiza distintas campañas de concienciación y guías informativas dirigidas tanto a individuos como a organizaciones, cuyo objetivo es ofrecer formación en ciberseguridad y autoprotección. El autor revisa también la eficacia de estas iniciativas, destacando que las intervenciones educativas deben diseñarse para llegar al público objetivo de manera clara y relevante, combinando el factor humano con medidas técnicas para garantizar su efectividad. No obstante, se identifican dificultades para evaluar la eficacia de estas estrategias centradas en las personas. La complejidad para medir su impacto real, junto con la falta de estudios empíricos sistemáticos, dificulta saber con certeza hasta qué punto estas medidas son efectivas en la reducción de la victimización.

En cuanto a la prevención centrada en la tecnología, el autor analiza las ventajas y limitaciones de las respuestas tecnológicas frente a las ciberestafas. Estas medidas incluyen herramientas que dificultan el contacto con la víctima, como filtros antispam, bloqueos de dominios asociados con sitios web de *phishing* y sistemas de advertencias disuasorias. Asimismo, se examinan tecnologías que buscan reducir los beneficios económicos obtenidos por los estafadores, mediante la implementación de capas adicionales de seguridad. Sin embargo, estas soluciones también presentan limitaciones como el coste elevado de implementación y mantenimiento, la falta de adopción generalizada, especialmente en pequeñas empresas y la necesidad de capacidad computacional avanzada para su funcionamiento óptimo. Por ello, al igual que ocurre con las es-

trategias centradas en el factor humano, las medidas tecnológicas también enfrentan dificultades en su evaluación. La ausencia de datos y la falta de intercambio de información entre organizaciones públicas y privadas dificultan determinar qué soluciones son más efectivas o rentables para reducir la victimización.

Expone el Prof. Steven Kemp que resulta sorprendente que, a pesar de la importante inversión de las organizaciones en ciberseguridad, apenas se haya investigado qué medidas ofrecen mejores resultados. Esta falta de evaluaciones rigurosas representa una laguna significativa en la prevención del fraude digital.

Como conclusiones del capítulo se señala la necesidad de combinar medidas centradas en el factor humano con soluciones tecnológicas. Ambas perspectivas deben actuar de manera complementaria, dado que las últimas resultan insuficientes por sí solas para prevenir eficazmente las ciberestafas.

En el último capítulo, se ofrecen una serie de reflexiones finales sobre la evolución y las perspectivas futuras de las ciberestafas, subrayando la importancia de anticiparse a los desafíos emergentes y la necesidad de fortalecer la investigación empírica y la colaboración institucional para abordar este fenómeno creciente.

El autor analiza cómo la introducción de tecnologías avanzadas, como las *Deepfakes* y los *chatbots* de inteligencia artificial generativa, está transformando el panorama de las ciberestafas. Aunque el uso de estas herramientas para cometer fraudes todavía se encuentra en una etapa incipiente, ya se han documentado casos en los que estas tecnologías han facilitado ataques sofisticados dirigidos a individuos y organizaciones. En particular, el autor advierte que la proliferación de herramientas como *chatbots* generativos puede permitir a los delincuentes llevar a cabo ataques más persuasivos y adaptados a una amplia variedad de víctimas. La capacidad de generar contenido sintético realista incrementa la eficacia de los engaños.

Ante este panorama, se destacan dos líneas de actuación fundamentales. Por un lado, la formación y concienciación, capacitando a los usuarios para que puedan adoptar una actitud crítica y reflexiva ante cualquier solicitud que reciban a través de las TIC, especialmente aquellas que involucren información confidencial o acciones financieras. Por otro lado, las instituciones deben implementar procedimientos de verificación adicionales que minimicen las oportunidades para la comisión de fraudes.

Asimismo, en la obra se señala la responsabilidad compartida entre las instituciones públicas y las empresas tecnológicas en la prevención y mitigación de las ciberestafas. El autor destaca el papel de la Comisión Europea en el desarrollo de normativas y directivas que garanticen una mayor seguridad en el entorno digital. Además, las empresas TIC tienen un rol crucial al diseñar y ofrecer productos y servicios que reduzcan las vulnerabilidades y no expongan a los usuarios a riesgos innecesarios.

En cuanto a los retos y oportunidades en el futuro de los estudios sobre las ciberestafas, el autor identifica la escasez de datos disponibles, especialmente en el contexto español, como uno de los mayores obstáculos para el avance del conocimiento sobre las ciberestafas. La falta de información rigurosa y detallada impide realizar un análisis adecuado de las tendencias delictivas y limita la capacidad de las instituciones para prevenir y reaccionar de manera eficaz ante este fenómeno.

Para abordar estas limitaciones, se subraya la necesidad de promover investigaciones empíricas a nivel global, con especial atención a contextos como España y Latinoamérica, donde, si bien las ciberestafas están ampliamente extendidas, los conocimientos sobre este fenómeno siguen siendo muy básicos. Para ello, se propone una colaboración activa entre universidades, instituciones públicas y organizaciones privadas como vía esencial para superar estas barreras. El intercambio de datos, la financiación conjunta y el desarrollo de proyectos de investigación interdisciplinarios son indispensables para generar un conocimiento más profundo sobre las ciberestafas y sus consecuencias. Expone el autor, que solo a través de esta colaboración será posible enfrentar un problema delictivo que no solo genera daños económicos y psicológicos, sino que continúa en aumento y ha demostrado estar para quedarse.

Por último, para concluir la reseña, es necesario destacar que la presente obra sobresale no solo por su profundidad, sino también por la rigurosidad metodológica con la que el autor aborda el fenómeno de las ciberestafas. A lo largo de sus capítulos, se desarrolla un análisis integral y bien fundamentado, sustentado en investigaciones empíricas tanto nacionales como internacionales y en los datos estadísticos más relevantes disponibles.

Entre las fortalezas más notables de la obra, destaca su capacidad para ofrecer una revisión exhaustiva de los aspectos clave en el abordaje integral de las ciberestafas. El autor no se limita a una mera descripción del delito; por el contrario, profundiza en el estudio de los autores, sus motivaciones y estructuras organizativas, así como en el análisis de las víctimas, sus perfiles y las consecuencias de este tipo de delitos. A ello se

añade un valioso examen de las estrategias de prevención, tanto desde el factor humano como desde las respuestas tecnológicas, logrando así un enfoque holístico y completo del problema.

En consecuencia, la obra se convierte en una lectura de gran utilidad tanto para quienes se inician en la temática de las ciberestafas, al proporcionarles una visión general del fenómeno, como para lectores especializados, quienes encontrarán en ella una oportunidad para actualizarse y explorar nuevas líneas de investigación.

El interés del autor por la materia resulta indiscutible, reflejado en la inclusión de lecturas complementarias y referencias bibliográficas al final de cada capítulo, lo que permite al lector profundizar en los temas tratados. La obra pone de manifiesto un trabajo rigurosamente documentado y el compromiso del autor por abordar con seriedad y profundidad una problemática de creciente relevancia social y económica. Por todo ello, y en virtud de su trayectoria científica y el interés demostrado en la materia, puede afirmarse que el Prof. Steven Kemp es, sin duda, la persona idónea para llevar a cabo una monografía de esta envergadura, como ha quedado sobradamente acreditado a lo largo de la obra.

Suscripción anual (tres números): 155 € (iva incluido)
Número suelto: 60 € (iva incluido)

Dykinson, S.L.

C/ Melendez Valdes, 61 – 28015 Madrid
Telfs. 91 544 28 69 / 91 544 28 46 – Fax 91 544 60 40
info@dykinson.com – www.dykinson.com – www.dykinson-on-line.com