UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

FRAUDE ORGANIZADO

DOCUMENTO TEMÁTICO

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO

FRAUDE ORGANIZADO

DOCUMENTO TEMÁTICO

NACIONES UNIDAS
Viena, 2024

Agradecimientos

El presente documento temático ha sido elaborado por la Sección de Apoyo a la Conferencia de la Subdivisión de Lucha contra la Delincuencia Organizada y el Tráfico Ilícito de la División de Tratados de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC).

Investigación y redacción

El presente documento temático fue redactado por Michael Skidmore, consultor. La UNODC desea agradecer las aportaciones de Ramy Abdelhady, Victoria Luján Ecarri, Roxana-Andreea Mastor y Riikka Puttonen de la Sección de Apoyo a la Conferencia, que contribuyeron a la elaboración del documento temático. El documento temático se benefició de las valiosas contribuciones de muchos miembros del personal de la UNODC, que examinaron varias secciones y aportaron sus perspectivas; entre estos integrantes del personal cabe mencionar a Loide Aryee, Renata Delgado-Schenk, Giovanni Gallo, Magdalena Howland, Theodore Leggett, Glen Prichard, Jason Reichelt, Tim Steele y Woody Tan.

Contribuciones

Otras personas y organizaciones contribuyeron a la elaboración de este documento temático. La UNODC expresa su profundo agradecimiento a quienes transmitieron sus conocimientos especializados y su experiencia durante la reunión internacional de expertos celebrada en forma presencial en Viena y en línea del 4 al 6 de marzo de 2024: Jorij Abraham (Global Anti-Scam Alliance), Bina Bhardwa (Institute for Crime and Justice Policy Research), Muhammad Bin Mohamed Farid (Singapur), Sebastian Bley (Agencia de la Unión Europea para la Cooperación Policial), Mark Button (Universidad de Portsmouth, Reino Unido de Gran Bretaña e Irlanda del Norte), Mina Chiang (Humanity Research Consultancy), Nicholas Court (Organización Internacional de Policía Criminal (INTERPOL)), Ian Dyson (Reino Unido), Richard Goldberg (Estados Unidos de América), Cosmin-Adrian Iordache (Fiscalía Europea), Eric Kasper (Humanity Research Consultancy), Jeanette Kroes (INTERPOL), Dexter Laggui (Filipinas), Michael Levi (Universidad de Cardiff, Reino Unido), Nicholas Lord (Universidad de Manchester, Reino Unido), Mary Rose Magsaysay (Filipinas), Rafael Henrique Martins Fernandes (Brasil), Jennifer Mendez (American Society of International Law), Daniel Mostardeiro Cola (Brasil), Olegs Olins (Letonia), Christopher Omahi Ogbaji (Nigeria), Sophia Rowe (Jamaica), Kien Soloman (Reino Unido), Victoria Ugo-Ali (Nigeria), Dan Joshua Valenton (Filipinas), Thomas Von der Gathen (Payment Services Austria), Xiumei Wang (Universidad Normal de Beijing), Kathy Waters (Advocating Against Romance Scammers) y Robin Tim Weis (Zero Project).

El Gobierno del Reino Unido realizó una contribución financiera para la publicación del presente documento temático. El contenido del documento temático es responsabilidad exclusiva de la UNODC y no refleja necesariamente los puntos de vista del Gobierno del Reino Unido.

Producción editorial: Sección de Publicaciones, Oficina de las Naciones Unidas en Viena.

ÍNDICE

Introducción

El fraude ha cambiado mucho con los años, adaptándose a los avances tecnológicos y a las transformaciones de la sociedad. Se ha vuelto cada vez más sofisticado y a menudo utiliza la manipulación psicológica, facilitada por las tecnologías de la información y las comunicaciones. El elevado volumen del fraude y su gravedad plantean un riesgo considerable para las personas, para las economías y para la prosperidad en todo el mundo y repercuten negativamente en la confianza de la población en el estado de derecho. Sin embargo, existen varias dificultades a la hora de elaborar un perfil preciso del fraude. A menudo, las víctimas no lo denuncian suficientemente debido a sentimientos de vergüenza o culpa, o por no reconocer que se ha producido un delito[1]. Además, una parte considerable del fraude está dirigido contra empresas, muchas de las cuales optan por no denunciar estos delitos para evitar dañar su reputación[2]. El anonimato y la lejanía que a menudo están asociados a la comisión de fraudes ocultan la identidad de los delincuentes a las víctimas y a las autoridades, lo que dificulta las gestiones para analizar los patrones subyacentes, los factores de vulnerabilidad y los riesgos asociados. Además, la naturaleza dinámica del fraude, que se adapta constantemente a los cambios en los sistemas jurídicos, sociales, comerciales y tecnológicos, hace que los métodos nuevos e innovadores que adopta puedan pasar desapercibidos dentro de los datos oficiales estáticos. En muchos casos, las entidades nacionales encargadas de hacer cumplir la ley no tienen capacidad para investigar y descubrir a los delincuentes y grupos delictivos organizados que están detrás del delito[3]: se requiere cooperación internacional, lo que indica que es necesario dar mayor relevancia al fraude en el marco de políticas y en la legislación contra la delincuencia organizada[4].

La comunidad internacional ha reconocido la preocupante magnitud del fraude y la necesidad de aunar esfuerzos para prevenirlo y combatirlo[5]. La Asamblea General, en su resolución 78/229, reafirmó la importancia de la labor de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en cumplimiento de su mandato en materia de prevención del delito y justicia penal, en particular prestar a los Estados Miembros que lo solicitan, con carácter prioritario, servicios de cooperación técnica, servicios de asesoramiento y otras modalidades de asistencia, y trabajar en coordinación con todos los órganos y oficinas pertinentes y competentes de las Naciones

[1] Mark Button, Christopher Lewis y Jacki Tapley, "Not a victimless crime: the impact of fraud on individual victims and their families", *Security Journal*, vol. 27, núm. 1 (febrero de 2014).

[2] Cynthia Courtois e Yves Gendron, "Research: why corporate fraud reports are down", *Harvard Business Review*, 1 de julio de 2020.

[3] El análisis de los datos sobre delincuencia en el Reino Unido de Gran Bretaña e Irlanda del Norte incluyó los vínculos entre los delitos de fraude denunciados por el público y la delincuencia organizada y estimó que al menos el 31% podía atribuirse a la delincuencia organizada. Esto se basó en varias características, incluida la participación de coautores, la reincidencia, el robo de grandes sumas de dinero y el nivel de sofisticación (p. ej., planificación o habilidad técnica). Sin embargo, la interpretación se ve dificultada por la limitada información contextual sobre los delincuentes y los procesos delictivos subyacentes y la falta de claridad conceptual para delimitar claramente el fraude que puede atribuirse a la delincuencia organizada (véase Ruth Crocker *et al.*, *The Impact of Organized Crime in Local Communities* (Londres, The Police Foundation, 2017)).

[4] Hans-Jörg Albrecht, "Police, policing and organized crime: lessons from organized crime research", en *European Law Enforcement Research Bulletin*, Special Conference Edition, núm. 2, Detlef Nogala *et al.*, eds. (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2017); y Michael Levi, Ognian Shentov y Boyko Todorov, eds., *Financing of Organised Crime* (Sofía, Center for the Study of Democracy, 2015).

[5] Véanse las resoluciones del Consejo Económico y Social 2004/26, 2007/20, 2009/22, 2011/35 y 2013/39, relativas a la cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad.

Unidas, y complementar su labor en relación con todas las formas de delincuencia organizada, incluido el fraude. Sin embargo, la intersección entre el fraude y la delincuencia organizada no se conoce bien y se ve aún más complicada por los solapamientos con otros ámbitos clave, como la ciberdelincuencia, la delincuencia de cuello blanco, el blanqueo de dinero y la corrupción[6]. Es necesario comprender el fraude organizado para fundamentar las decisiones de los encargados de formular políticas y otras partes interesadas e impulsar respuestas eficaces. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, principal instrumento mundial jurídicamente vinculante para prevenir y combatir todas las formas y manifestaciones de la delincuencia organizada transnacional y proteger a sus víctimas, proporciona un marco para comprender la naturaleza del fraude organizado y la manera en que la respuesta a ese delito puede integrarse en la que se da a las distintas amenazas que presenta la delincuencia organizada transnacional.

Alcance del documento temático

El fraude es una categoría delictiva muy amplia. Uno de los mayores retos para comprenderlo es su alcance. Abarca una serie de conductas delictivas que comparten el principio común de la deshonestidad. Las oportunidades de emplear la deshonestidad con fines de fraude comprenden toda la gama de entornos sociales, comerciales, financieros y tecnológicos, que pueden variar en las distintas regiones del mundo[7]. Estas oportunidades son aprovechadas por delincuentes de entornos muy diversos, desde profesionales que se aprovechan de una posición legítima en una empresa hasta ciberdelincuentes procedentes de comunidades desfavorecidas[8]. De este modo, el fraude se distingue de muchas otras categorías de delitos que abarcan conductas delictivas más definidas que tienen lugar en entornos específicos (p. ej., el robo con allanamiento de morada). Esta diversidad plantea dificultades a la hora de elaborar una imagen única, cohesionada y completa del fraude.

El presente documento temático se refiere al fraude perpetrado por grupos delictivos organizados (es decir, el fraude organizado). El papel de la delincuencia organizada puede variar en función del tipo de fraude, aunque, en mayor o menor medida, está implicada en casi todos los tipos de fraude. A efectos de limitar el alcance del documento temático, no se incluye en él lo siguiente:

- Otros delitos en los que el fraude desempeña un papel facilitador, incluido el uso fraudulento de la identidad para impedir que se localice al autor, como la apertura de cuentas financieras para blanquear el producto del delito[9]; comunicaciones fraudulentas para entablar una relación con una víctima con el fin de chantajearla o extorsionarla con miras

[6] Jay S. Albanese, "Organized crime as financial crime: the nature of organized crime as reflected in prosecutions and research", *Victims and Offenders*, vol. 16, núm. 3 (2021); y Andrea Di Nicola, "Towards digital organized crime and digital sociology of organized crime", *Trends in Organized Crime* (2022).

[7] Michael Levi, "Organized fraud and organizing frauds: unpacking research on networks and organization", *Criminology and Criminal Justice*, vol. 8, núm. 4 (noviembre de 2008). Véase también Organización Internacional de Policía Criminal (INTERPOL), "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas" (Lyon (Francia), 2024).

[8] Véanse, por ejemplo, Arjan Reurink, *Financial Fraud: A Literature Review*, MPIfG Discussion Paper, núm. 16/5 (Colonia (Alemania), Instituto Max Planck para el Estudio de las Sociedades, 2016); y Mikol A. Mortley, "A crime of opportunity: an analysis of the Jamaican lottery scam" (Kingston, 2017).

[9] Simon Baechler, "Document fraud: will your identity be secure in the twenty-first century?", *European Journal on Criminal Policy and Research*, vol. 26, núm. 3 (septiembre de 2020).

a obtener dinero[10], y anuncios de empleo fraudulentos dirigidos a captar víctimas y someterlas a la trata con fines de trabajo forzoso y servidumbre[11].

- El fraude dirigido contra los intereses financieros del Estado (p. ej., regímenes fiscales), como el fraude intracomunitario del operador desaparecido (también conocido como fraude del IVA o fraude carrusel); el fraude en el ámbito de los impuestos especiales, en el que no se pagan los impuestos sobre productos importados (p. ej., combustible); el fraude en la contratación pública, y las solicitudes fraudulentas de subvenciones y subsidios gubernamentales[12]. El panorama de políticas y respuestas ante estos tipos de fraude puede ser distinto, ya que está formado por diversas agencias y poderes reguladores más allá de los organismos encargados de hacer cumplir la ley (p. ej., la autoridad fiscal)[13]. Los vínculos entre estos tipos de fraude y la delincuencia organizada están mejor establecidos en la bibliografía[14].

Este documento temático se centra en el fraude organizado dirigido contra particulares o instituciones privadas con el fin de obtener un beneficio económico u otro beneficio de orden material.

Metodología

Desarrollo de una tipología

Son muchos los principios que pueden adoptarse para representar las distintas dimensiones del fraude. Estos pueden incluir los principales facilitadores técnicos o delictivos subyacentes que proporcionan las herramientas para perpetrar el fraude, como los métodos clave para aprovecharse de canales de comunicación como las telecomunicaciones o la publicidad en línea[15], y los procesos de piratería informática, usurpación de identidad o ingeniería social[16]. Ordenar el conocimiento del fraude de acuerdo con estos principios puede proporcionar información sobre los procesos subyacentes que impulsan la conducta fraudulenta delictiva; sin embargo, la visibilidad de estos distintos elementos puede ser limitada. Esto se debe a que las víctimas que denuncian los delitos a menudo no saben cómo se perpetró el fraude[17]. Además, algunos factores subyacentes facilitan múltiples formas de delincuencia; por ejemplo, la piratería informática y la intrusión en un sistema pueden ser precursores del fraude, pero también de otras categorías de delitos (p. ej., el chantaje mediante ataques con programas secuestradores).

---

[10] Anna Coluccia *et al.*, "Online romance scams: relational dynamics and psychological characteristics of the victims and scammers – a scoping review", *Clinical Practice and Epidemiology in Mental Health*, vol. 16 (2020).

[11] *Global Report on Trafficking in Persons 2022* (publicación de las Naciones Unidas, 2022), pág. 102. Para más información, véanse la sección sobre fraude relacionado con el empleo en el capítulo II del presente documento temático; e INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 20.

[12] Shann Hulme, Emma Disley y Emma Louise Blondes, eds., *Mapping the Risk of Serious and Organised Crime Infiltrating Legitimate Businesses: Final Report* (Bruselas, Oficina de Publicaciones, 2021); Agencia de la Unión Europea para la Cooperación Policial (Europol), *Serious and Organised Crime Threat Assessment: Crime in the Age of Technology* (La Haya, 2017); y Europol, *Online Fraud Schemes: A Web of Deceit*, Europol Spotlight Report Series (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2023).

[13] Mark Button, David Shepherd y Dean Blackbourn, *The Fraud "Justice Systems": A Scoping Study on the Civil, Regulatory and Private Paths to "Justice" for Fraudsters – Main Report* (Portsmouth (Reino Unido), Universidad de Portsmouth, 2016).

[14] Hulme, Disley y Blondes, eds., *Mapping the Risk of Serious and Organised Crime*.

[15] Por ejemplo, David Ng'ang'a Njuguna, John Kamau y Dennis Kaburu, "A review of smishing attacks mitigation strategies", *International Journal of Computer and Information Technology*, vol. 11, núm. 1 (febrero de 2022); Jean-Loup Richet, "How cybercriminal communities grow and change: an investigation of ad-fraud communities", *Technological Forecasting and Social Change*, vol. 174, art. núm. 121282 (enero de 2022); y Shadi Sadeghpour y Natalija Vlajic, "Ads and fraud: a comprehensive survey of fraud in online advertising", *Journal of Cybersecurity and Privacy*, vol. 1, núm. 4 (diciembre de 2021).

[16] Jason R. C. Nurse, "Cybercrime and you: how criminals attack and the human factors that they seek to exploit", en *The Oxford Handbook of Cyberpsychology*, Alison Attrill-Smith *et al.*, eds. (Oxford (Reino Unido), Oxford University Press, 2019).

[17] Mark Button *et al.*, "Online frauds: learning from victims why they fall for these scams", *The Australian and New Zealand Journal of Criminology*, vol. 47, núm. 3 (diciembre de 2014).

Las categorías de fraude definidas para el presente documento temático adoptan una perspectiva centrada en la víctima y, por tanto, se refieren principalmente a la narrativa o artimaña que se presenta a las víctimas (p. ej., la inversión o el romance). En este contexto, el documento temático se basa en trabajos anteriores que han adoptado principios similares para desarrollar una tipología del fraude basada en las víctimas y sus experiencias, como una tipología que refleje la recompensa, el beneficio o el resultado que la víctima espera obtener a partir de la comunicación fraudulenta o que se le ha prometido en ella[18]. Los métodos subyacentes a las categorías basadas en las víctimas tienen puntos en común, en cuanto a las tecnologías y técnicas utilizadas para perpetrar el engaño por los delincuentes implicados en los distintos tipos de fraude. Algunos delincuentes pueden cometer varios tipos de fraude como parte de un mismo plan o emplear técnicas similares para cometer distintos tipos de fraude.

Una categoría incluida en la tipología es el fraude dirigido a empresas y organizaciones. Esto refleja una categoría de víctima más que una narrativa o artimaña específica, y por lo tanto incorpora diversos planes y métodos de fraude. Estos tipos de fraude se consolidaron a fin de reconocer a las empresas y organizaciones como un grupo clave de víctimas.

Estas categorías se presentan como un paso inicial para desarrollar un lenguaje y una comprensión comunes de las diferentes categorías de fraude organizado. Estas categorías no son necesariamente propias de los grupos delictivos organizados, pero cada una de ellas se analizará en el contexto del fraude organizado. Algunas son más amplias que otras y abarcan múltiples subcategorías, algunas de las cuales se analizan de forma no exhaustiva en el documento temático.

Examen de la bibliografía

En este documento temático se presenta una investigación exploratoria dirigida a examinar la naturaleza del fraude organizado que se hace presente en distintas regiones del mundo. Contiene una recopilación y un examen de información procedente de artículos de revistas académicas, documentos de política y publicaciones.

Se realizó una búsqueda de fuentes en línea para encontrar publicaciones que tratasen sobre los delitos de fraude organizado o sus autores. La cobertura del tema del fraude organizado, o de la delincuencia organizada en el contexto del fraude, ha sido limitada en la bibliografía existente. El documento temático contiene una síntesis de las pruebas recogidas en múltiples ámbitos de la criminología relacionados entre sí, incluidos el fraude, la delincuencia organizada y la ciberdelincuencia. El documento no contiene un examen sistemático de la bibliografía, sino que es más bien un análisis selectivo de las obras más importantes dirigido a representar e ilustrar algunos de los temas principales.

Estudios de casos

Se recopilaron estudios de casos para ofrecer ejemplos ilustrativos del fraude organizado en las distintas regiones del mundo y captar métodos y tecnologías nuevos y emergentes. Los estudios de casos proceden de diversas fuentes, como el portal de gestión de conocimientos Intercambio de

[18] El documento temático se basa en investigaciones anteriores que han tratado de delimitar las diferentes categorías de fraude dirigido a particulares o empresas, como Michaela Beals, Marguerite DeLiema y Martha Deevy, "Framework for a taxonomy of fraud" (Stanford (California, Estados Unidos), Stanford Center on Longevity, 2015); y Michael Levi y John Burrows, "Measuring the impact of fraud in the UK: a conceptual and empirical journey", *The British Journal of Criminology*, vol. 48, núm. 3 (mayo de 2008).

Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC), artículos académicos, informes de política e investigaciones jurídicas.

Se llevó a cabo una investigación preliminar sobre la legislación en materia de fraude en 37 países de todas las regiones del mundo, en la que se prestó especial atención a las definiciones y marcos jurídicos que orientan las decisiones sobre la imposición de penas a los delincuentes condenados. Puede haber elementos relacionados con el fraude en la legislación de otros países que no se examinan en este documento.

Limitaciones del examen

En muchas fuentes oficiales y trabajos de investigación, el fraude se examina a través del prisma de la aplicación de la ley y los datos oficiales. Muchas veces, los casos de fraude no se denuncian y, por lo tanto, es necesario actuar con cautela a la hora de interpretar el problema y desarrollar soluciones sobre la base de datos incompletos. El presente documento temático contiene una recopilación de investigaciones de diversas regiones, pero la disponibilidad de esas investigaciones era variada y en algunas regiones eran más limitadas o incipientes. Por consiguiente, se desconoce hasta qué punto los datos incluidos en el documento temático representan las tendencias del fraude organizado en todas las regiones. También existe actualmente un vacío en los datos sobre el fraude organizado desglosados por factores como la discapacidad, la edad, el género y la situación económica, lo que limita el análisis y la comprensión de los elementos que hacen más fácil captar víctimas y perpetrar actos de fraude organizado.

Estructura del documento temático

El documento temático tiene la siguiente estructura:

- En el capítulo I se establecen los principios para entender el fraude organizado y se examinan la definición de fraude y los aspectos clave de la Convención contra la Delincuencia Organizada.
- En el capítulo II se presenta una tipología del fraude organizado, con una descripción pormenorizada de cada categoría.
- El capítulo III contiene un análisis de los autores de delitos de fraude organizado, con un examen de sus perfiles y las vías que los llevan a cometerlos.
- El capítulo IV contiene una descripción de los facilitadores transversales del fraude, incluidas algunas de las tecnologías y comportamientos clave que posibilitan el fraude organizado.
- En el capítulo V se analizan las respuestas nacionales e internacionales, las consideraciones clave, las lagunas y los ámbitos en los que se puede mejorar la prevención y la aplicación de la ley.

CAPÍTULO I

Principios para comprender el fraude organizado

Antes de centrarse en la tipología del fraude organizado, el presente capítulo aborda algunas consideraciones de carácter general en torno a la definición de fraude, la Convención contra la Delincuencia Organizada y el fraude en el contexto de la delincuencia organizada.

Definición de fraude

No existe una forma única y definitiva de concebir las conductas que constituyen fraude. El fraude se ha definido en sentido muy amplio, por ejemplo, como la obtención de algo de valor o la elusión de una obligación mediante engaño[19]. También se han proporcionado definiciones más elaboradas para describir en términos más específicos las conductas compuestas que representa el fraude, entre los que destacan la intención deliberada y la violación de la confianza[20]. INTERPOL ha hecho hincapié en el elemento deliberado implícito en el término "engaño", reforzando la importancia de la intención a la hora de definir el fraude, que define como actividades "destinadas a obtener un lucro a través de acciones deliberadas y engañosas contra personas y en su detrimento"[21].

Del mismo modo, no existe una única definición de fraude en la legislación, y las distintas definiciones en jurisdicciones legales o estatutos diferentes evocan solo un concepto amplio[22]. En la legislación penal de los países, el fraude se describe de diferentes maneras y con distintos grados de especificidad[23]. Algunas leyes ofrecen una descripción generalizada de las conductas que constituyen fraude[24], mientras que otras hacen referencia a determinadas actividades, productos o servicios que se destacan en las tramas fraudulentas, como la suplantación de una entidad fiable o la manipulación o el uso no autorizado de datos[25]. Algunos Estados han establecido legislación diferenciada para combatir distintas facetas del delito de fraude, por ejemplo, el fraude informático, el fraude crediticio o el fraude contra empresas o en subastas[26].

---

[19] Grace Duffield y Peter Grabosky, *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, núm. 199 (Canberra, Instituto Australiano de Criminología, 2001), pág. 1. Véase también Michael Levi, "Financial crimes", en *Oxford Handbook of Crime and Public Policy*, Michael Tonry, ed. (Nueva York, Oxford University Press, 2009), págs. 223 a 246.

[20] Reurink, *Financial Fraud*.

[21] INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 5.

[22] Alan Doig, *Fraud* (Cullompton (Reino Unido), Willan, 2006); y Reurink, *Financial Fraud*.

[23] A efectos del presente documento, se examinaron las definiciones jurídicas de 37 países de todas las regiones del mundo.

[24] Véanse, por ejemplo, los ejemplos de legislación de España y el Uruguay incluidos en la presente sección.

[25] Por ejemplo, en Argelia, el fraude se define como la recepción de dinero utilizando una identidad falsa o los nombres de otras personas, como las autoridades, o convenciendo a una persona de algo que no es cierto, como que ha ganado la lotería o que ha ocurrido un accidente.

[26] Por ejemplo, en la República de Corea existe legislación separada sobre el fraude que perjudica el crédito de otra persona y sobre el fraude mediante el uso de una computadora (p. ej., la introducción de datos falsos para la falsificación de identidad).

Hay algunos elementos básicos del fraude que figuran en la mayoría de las definiciones jurídicas: el uso del engaño para obtener una ventaja o beneficio injustos y la provocación de un perjuicio a otra persona u organización. El engaño se describe de formas diferentes como la conducta deshonesta, la representación falsa o engañosa, las artimañas, el artificio, las maniobras fraudulentas, el abuso de confianza o la ocultación u omisión de información. El perjuicio para otro está en muchos casos implícito en el beneficio para los autores del delito, pero en algunas definiciones esto se resalta utilizando términos como los referidos a afectar o perjudicar los intereses financieros de otros, una pérdida ilícita o la referencia al objeto de fraude. El perjuicio puede ser para un particular, una empresa o un Estado.

A continuación se ofrecen las definiciones de "estafa" que figuran en la legislación de España y el Uruguay, que constituyen ejemplos de dos concepciones amplias de fraude que se han adoptado en la legislación.

EJEMPLO DE LEGISLACIÓN: ESPAÑA

LEY ORGÁNICA 10/1995: CÓDIGO PENAL

Artículo 248. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

EJEMPLO DE LEGISLACIÓN: URUGUAY

CÓDIGO PENAL NÚM. 9155

Artículo 347. El que con estratagemas o engaños artificiosos indujere en error a alguna persona, para procurarse a sí mismo o a un tercero, un provecho injusto, en daño de otro, será castigado con seis meses de prisión a cuatro años de penitenciaría.

En el presente documento temático se adopta una definición amplia de fraude, a fin de abarcar las variantes descritas en la legislación de los distintos países. Incluye el fraude que utiliza deliberadamente el engaño[27], por cualquier método[28] o medio[29], con la intención de obtener un beneficio económico ilícito u otro beneficio de orden material[30], y que causa un perjuicio a otro[31].

Una última cuestión que debe tenerse en cuenta a la hora de definir el fraude es la delgada línea que puede separar un asunto penal de uno civil —especialmente en los casos en que la intención es difícil de discernir— y las dificultades con que pueden tropezar las entidades encargadas de hacer cumplir la ley para determinar que se ha producido un delito[32]. Además, un autor puede ser castigado con

[27] Esto incluye el uso de nombres, cualidades o empresas falsas o la realización de declaraciones falsas que abusen de la confianza e infundan seguridad, una falsa esperanza o temor de un acontecimiento que no es real para inducir a otra persona a desprenderse de dinero propio o ajeno o a renunciar a un derecho legal o de propiedad o a cualquier beneficio de orden material. Esto incluye también la ocultación deliberada de hechos materiales.

[28] Por ejemplo, mediante el uso de documentos falsos o introduciendo datos falsos o dando órdenes no autorizadas a una computadora.

[29] Esto incluye el fraude perpetrado en línea, por teléfono, por correo o en persona, o una combinación de estos medios.

[30] Esto incluye la obtención o el intento de obtener fondos, acceso a servicios, bienes muebles o inmuebles, bonos, letras, promesas, recibos o descargos o una liberación de obligaciones.

[31] Este perjuicio puede ser para una persona, una empresa o una organización e incluye pérdidas de cualquier valor o importancia para la víctima.

[32] A modo de ejemplo, en el contexto del fraude en las inversiones, la mala praxis puede ir desde el engaño propiamente dicho hasta las prácticas negligentes y el suministro de información deficiente a los clientes. Además, podría establecerse que el beneficio previsto se obtendría muchos años más tarde y, así, puede ser difícil demostrar que no se cumplirá lo prometido y, por lo tanto, establecer la existencia de una intención delictiva (Michael Skidmore, *Protecting People's Pensions: Understanding and Preventing Scams* (Londres, The Police Foundation, 2020)).

una serie de sanciones penales, civiles o administrativas en función de la naturaleza del fraude y de las disposiciones reglamentarias aplicables en el sector público o privado[33]. Dado que se centra en la delincuencia organizada, el presente documento aborda el fraude por el que existe responsabilidad penal, pero se señala que habrá diferencias en las distintas jurisdicciones nacionales[34].

El tema más amplio de la ciberdelincuencia ocupa un lugar destacado en el fraude, aunque no existe un enfoque único para definir el fraude en el contexto de la ciberdelincuencia[35]. Una forma de entender la ciberdelincuencia es examinar cómo y en qué medida un delito ha sido transformado por las tecnologías de la información y las comunicaciones[36]. El fraude relacionado con estas tecnologías suele describirse como un delito facilitado por la cibernética, en el sentido de que es un delito tradicional que utiliza los sistemas de tecnologías de la información y las comunicaciones para ganar mayor magnitud y alcance[37]. Por lo tanto, es diferente de los delitos basados en la cibernética, que solo pueden cometerse mediante el uso de sistemas de tecnologías de la información y las comunicaciones y cuyo objetivo es la integridad, disponibilidad y confidencialidad de esos sistemas y de los datos electrónicos[38]. Sin embargo, esta dicotomía no tiene en cuenta las diversas formas en que la delincuencia basada en la cibernética se entrecruza con el fraude, en particular desde la perspectiva de los delincuentes y la secuencia de delitos subyacentes en la comisión del fraude, por ejemplo, obtener acceso ilegal a un sistema de tecnologías de la información y las comunicaciones para perpetrar un fraude de vulneración del correo electrónico empresarial. Existen marcos que conceptualizan la ciberdelincuencia como un espectro continuo, que va desde los delitos totalmente basados en la tecnología hasta los delitos en los que el uso de sistemas de tecnologías de la información y las comunicaciones es accesorio[39]. El uso de los sistemas de tecnologías de la información y las comunicaciones para cometer fraude es muy variable y abarca gran parte de ese espectro. El presente documento temático contiene el término "ciberfraude", que representa todos los tipos de fraude de ese espectro.

Grupos delictivos organizados en el contexto del fraude

El fraude engloba delitos de muy diversa índole en cuanto a métodos, complejidad e impacto. Abarca a delincuentes que van desde oportunistas que obtienen ganancias económicas moderadas hasta delincuentes muy motivados y organizados que hacen todo lo posible por orquestar el fraude para obtener niveles asombrosos de beneficios del delito[40]. Así pues, puede ser difícil trazar una línea que separe el fraude organizado de otros tipos de fraude. Por lo tanto, contar con distinciones más claras ayudaría a desarrollar políticas y respuestas que se ajusten más firmemente al problema designado.

En el artículo 2 a) de la Convención contra la Delincuencia Organizada se define un "grupo delictivo organizado" como un grupo estructurado de tres o más personas que exista durante cierto tiempo y que

---

[33] Mark Button *et al.*, *Fraud and Punishment: Enhancing Deterrence Through More Effective Sanctions – Main Report* (Portsmouth (Reino Unido), Universidad de Portsmouth, 2012).

[34] Reurink, *Financial Fraud*.

[35] Alisdair A. Gillespie y Samantha Magor, "Tackling online fraud", *ERA Forum: Journal of the Academy of European Law*, vol. 20. núm. 3 (2019).

[36] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge (Reino Unido); Malden (Massachusetts, Estados Unidos), Polity Press, 2007).

[37] Los términos "delito facilitado por la cibernética" y "delito basado en la cibernética" se utilizan únicamente con fines ilustrativos. No existe un acuerdo internacional sobre su contenido y uso exactos.

[38] Pueden encontrarse ejemplos de delitos facilitados por la cibernética y de delitos basados en la cibernética en Mike McGuire y Samantha Dowling, *Cyber Crime: A Review of the Evidence – Summary of Key Findings and Implications*, Home Office Research Report, núm. 75 (2013).

[39] Sarah Gordon y Richard Ford, "On the definition and classification of cybercrime", *Journal in Computer Virology*, vol. 2, núm. 1 (agosto de 2006); y Kirsty Phillips *et al.*, "Conceptualizing cybercrime: definitions, typologies and taxonomies", *Forensic Sciences*, vol. 2, núm. 2 (abril de 2022).

[40] Véanse también Jonathan M. Karpoff, "The future of financial fraud", *Journal of Corporate Finance*, vol. 66 (2021); y Levi, "Organized fraud and organizing frauds".

actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material. En el artículo 2 c) de la Convención también se aclara el significado de "grupo estructurado". Estas definiciones incluyen cierta flexibilidad para que las entidades encargadas de hacer cumplir la ley identifiquen y enfrenten a los grupos delictivos organizados. La Convención no especifica qué estructura debe tener un grupo ni durante cuánto tiempo debe haber existido[41].

Los delincuentes pertenecientes a grupos delictivos organizados se estructuran de diversas maneras. Entre estos grupos se incluyen los que funcionan con una jerarquía más rígida, los que tienen estructuras horizontales que se articulan en torno a un grupo central de individuos y las redes que implican alianzas cambiantes de delincuentes individuales que, si bien no se perciben a sí mismos como un grupo, quedan comprendidos en la definición.

Los atributos asociados convencionalmente al estereotipo de la delincuencia organizada no siempre son esenciales para la comisión de actos de fraude organizado[42] y los modelos de negocio y estructuras adoptados por los grupos delictivos organizados deben considerarse en relación con los entornos en los que surgen las oportunidades delictivas, los métodos utilizados y las aptitudes necesarias:

- El fraude se refiere principalmente al robo de dinero y no a la producción o distribución de bienes ilegales, lo que lo distingue de otras actividades de la delincuencia organizada.
- Muchas actividades fraudulentas se llevan a cabo a distancia, facilitadas por una tecnología que permite la comunicación anónima y la transferencia de fondos robados a través de fronteras nacionales, y rara vez es necesario que las víctimas y los delincuentes se encuentren en el mismo lugar al mismo tiempo.
- El fraude suele depender de que las víctimas faciliten voluntariamente el acceso a sus fondos, en lugar de utilizar la fuerza o la coacción, y el éxito depende de tácticas engañosas que pueden difuminar las fronteras entre entidades legítimas e ilegítimas.
- El fraude de cuello blanco se comete desde dentro de organizaciones u ocupaciones por lo demás legítimas.

No existe una estructura típica de un grupo delictivo organizado implicado en el fraude y, al igual que ocurre con otras formas de delincuencia organizada, hay variaciones regionales en los métodos y estructuras empleados por los grupos delictivos organizados[43]. Esto se debe, en parte, a la gran diversidad de oportunidades para cometer fraudes graves que surgen en entornos empresariales, financieros y comerciales globales e interconectados. La organización de estos delitos y sus autores adoptan formas muy diversas cuando los grupos delictivos organizados tratan de aprovechar esas oportunidades. La aparición de la delincuencia organizada en las distintas regiones refleja las relaciones contingentes entre los diferentes entornos globales, la capacidad de quienes desean cometer fraude en una población para identificar y aprovechar las oportunidades para delinquir y los controles establecidos por el Estado u otras entidades para prevenir esos delitos[44].

[41] En la bibliografía de investigación se aplican multitud de definiciones de delincuencia organizada, algunas de las cuales especifican actividades como la violencia, la corrupción o la infiltración en la economía legítima como elementos intrínsecos de la presencia de delincuencia organizada. Por ejemplo, un estudio destacaba la ausencia de estas actividades entre quienes cometían fraude cibernético y cuestionaba así el papel que desempeñaba la "delincuencia organizada" en esos delitos (Eric Rutger Leukfeldt, Anna Lavorgna y Edward R. Kleemans, "Organised cybercrime or cybercrime that is organised? An assessment of the conceptualization of financial cybercrime as organised crime", *European Journal in Criminal Policy and Research*, vol. 23, núm. 3 (septiembre de 2017)).

[42] Kim-Kwang Raymond Choo y Russell G. Smith, "Criminal exploitation of online systems by organised crime groups", *Asian Journal of Criminology*, vol. 3, núm. 1 (junio de 2008); Levi, "Organized fraud and organizing frauds"; y Di Nicola, "Towards digital organized crime".

[43] INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas".

[44] Levi, "Organized fraud and organizing frauds".

La investigación sobre las formas que adoptan los grupos delictivos organizados en el contexto del fraude aún está en desarrollo, pero comprender sus diferentes manifestaciones es un paso importante para identificar y priorizar a quienes cometen los fraudes más graves para la intervención de las entidades encargadas de hacer cumplir la ley[45].

La comisión de un fraude conlleva una compleja serie de acontecimientos relacionados con la planificación, ejecución y finalización de la actividad delictiva con el fin de acceder a los fondos y evitar ser detectado por las autoridades[46]. El fraude puede ser transnacional, producirse durante un período de tiempo prolongado, alcanzar a multitud de víctimas e implicar procesos de blanqueo de dinero y corrupción en los sectores público o privado[47]. A menudo se necesitan coautores para llevar a cabo la compleja serie de acontecimientos en su totalidad. A algunos se los contrata para que aporten capacidades específicas que puedan aumentar la capacidad y el alcance para cometer fraudes, mientras que a otros se les exige que realicen tareas intensivas en trabajo. Algunos ejemplos son la contratación de facilitadores profesionales legítimos, ciberdelincuentes con acceso a conocimientos y recursos técnicos y operadores telefónicos que se dedican al *telemarketing*[48]. Los coautores que forman parte de grupos delictivos organizados desempeñan diversas funciones que dependen de los requisitos específicos de un acto de fraude y pueden tener diferentes niveles de importancia, conocimiento del plan e implicación en él[49].

La naturaleza de las relaciones entre coautores dentro de los distintos grupos delictivos organizados puede diferir en función de cómo se establezcan y con qué fin. Algunos grupos delictivos organizados fomentan vínculos sociales duraderos entre los codelincuentes, mientras que en otros las relaciones se establecen con el propósito más singular y pragmático de cometer un delito[50]. El modo en que estas relaciones toman forma puede afectar a la estructura y estabilidad del grupo delictivo organizado y esta variación es evidente en el contexto del fraude organizado.

Los grupos delictivos organizados que se dedican a otras formas de delincuencia grave pueden sentirse atraídos por los grandes beneficios y los riesgos relativamente bajos que conlleva la comisión de fraudes[51]. Suelen ser grupos duraderos que pueden aprovechar sus vínculos y recursos delictivos para facilitar

---

[45] Es importante señalar que la comisión de un fraude grave no siempre está supeditada a la existencia de coautores. Por ejemplo, hay profesionales que abusan de una posición legítima o que son capaces de aprovechar la tecnología para automatizar el delito (Levi, "Organized fraud and organizing frauds"; y Wystke van der Wagen y Wolter Pieters, "From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks", *The British Journal of Criminology*, vol. 55, núm. 3 (mayo de 2015)).

[46] Por ejemplo, véanse Amanda Bodker *et al.*, "Card-not-present fraud: using crime scripts to inform crime prevention initiatives", *Security Journal*, vol. 36, núm. 4 (diciembre de 2022); Claire Seungeun Lee, "A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea", *Crime, Law and Social Change*, vol. 74, núm. 2 (septiembre de 2020); y Levi, "Organized fraud and organizing frauds".

[47] Por ejemplo, véanse Rutger Leukfeldt y Jurjen Jansen, "Cyber criminal networks and money mules: an analysis of low-tech and high-tech fraud attacks in the Netherlands", *International Journal of Cyber Criminology*, vol. 9, núm. 2 (diciembre de 2015); Michael Skidmore y Beth Aitkenhead, "Understanding the characteristics of serious fraud offending in the UK" (Londres, The Police Foundation, 2023); Olayinka Akanle, J. O. Adesina y E. P. Akarah, "Towards human dignity and the internet: the cybercrime (*yahoo yahoo*) phenomenon in Nigeria", *African Journal of Science, Technology, Innovation and Development*, vol. 8, núm. 2 (2016); y Tiggey May y Bina Bhardwa, *Organised Crime Groups Involved in Fraud*, Crime Prevention and Security Management Series (Londres, Palgrave Macmillan, 2018).

[48] Por ejemplo, véanse May y Bhardwa, *Organised Crime Groups Involved in Fraud*; Usman Adekunle Ojedokun y Ayomide Augustine Ilori, "Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria", *International Journal of Criminal Justice*, vol. 3 (2021); Jienan Liu *et al.*, "Understanding, measuring, and detecting modern technical support scams", en *8th Institute of Electrical and Electronics Engineers (IEEE) European Symposium on Security and Privacy*, ponencia presentada en el simposio celebrado en Delft (Reino de los Países Bajos), del 3 al 7 de julio de 2023; y Vaclav Jirovsky *et al.*, "Cybercrime and organized crime", en *ARES 18: Proceedings of the 13th International Conference on Availability, Reliability and Security*, art. núm. 61 (Hamburgo (Alemania), 2018).

[49] Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending"; y Neal Shover, Glenn S. Coffey y Clinton Robert Sanders, "Dialing for dollars: opportunities, justifications, and telemarketing fraud", *Qualitative Sociology*, vol. 27, núm. 1 (marzo de 2004).

[50] Esto distingue a los grupos delictivos organizados que adoptan "estructuras delictivas asociativas" de los que adoptan "estructuras delictivas empresariales" (Klaus von Lampe, *Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-legal Governance* (Los Ángeles (California, Estados Unidos), Sage Publications, 2016)).

[51] Un ejemplo ilustrativo es el de la denominada Black Axe Confraternity, un grupo delictivo organizado de larga tradición que surgió en Nigeria pero tiene miembros en varios países. Participan en varias formas de delincuencia organizada, entre ellos la trata de personas y el tráfico de drogas, así como en fraudes románticos y otras formas de ciberdelincuencia. Véanse Nate Allen, Matthew La Lime y Tomsin Sammer-Nlar, *The Downsides of Digital Revolution: Confronting Africa's Evolving Cyber Threats* (Ginebra, Global Initiative against Transnational Organized Crime, 2022); y Kim-Kwang Raymond Choo, "Organized crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, núm. 3 (septiembre de 2008).

la comisión de fraudes a gran escala. Esto puede incluir la capacidad de ejercer influencia sobre otras personas, tanto en la sociedad legítima como en el hampa[52]. En algunas regiones, los grupos delictivos organizados ofrecen protección y seguridad para aislar a las personas locales que cometen fraudes de la amenaza de las entidades locales encargadas de hacer cumplir la ley o de otros delincuentes[53]. Un ejemplo clave son los denominados complejos de estafas operados por grupos policriminales en Asia Sudoriental, que han industrializado procesos para perpetrar ciertos tipos de fraude (p. ej., fraudes románticos), en parte mediante la trata de víctimas a las que engañan o coaccionan para que cometan fraudes[54]. En algunos casos, los beneficios del fraude pueden ser utilizados por los grupos delictivos organizados para financiar otras actividades delictivas graves. El fraude puede figurar en el nexo entre la delincuencia organizada y el terrorismo, ya que proporciona los medios para financiar las actividades de organizaciones terroristas[55].

Muchos grupos delictivos organizados implicados en el fraude se forman con el único propósito de cometer estos delitos para obtener un beneficio ilícito. Las relaciones entre codelincuentes pueden tener su origen en estrechos vínculos sociales[56], pero también es habitual que surjan de mercados en los que se compran y venden conocimientos y recursos[57]. Esto fomenta acuerdos de colaboración fluidos, en los que los delincuentes se reúnen en torno a "proyectos" delictivos de duración limitada. Las relaciones entre los miembros del grupo pueden ser transaccionales o de corta duración, o pueden mantenerse solo mientras el plan fraudulento tenga éxito[58]. Algunos grupos delictivos organizados imitan estructuras de mano de obra legítima, con espacio de oficinas y coautores empleados como asalariados o contratados para prestar un servicio[59]. Sin embargo, la coautoría en el contexto del ciberfraude también puede tener su origen en relaciones establecidas en línea. Además de crear nuevas oportunidades delictivas para cometer fraudes[60], Internet ha reducido las barreras para entablar relaciones con nuevos posibles coautores: ha creado entornos más accesibles en los que delincuentes nuevos y anónimos pueden establecer rápidamente relaciones de confianza y aprovechar el capital delictivo disponible en las redes en línea[61]. Un ejemplo

[52] Además de formarse sobre la base de vínculos sociales, algunos grupos pueden adoptar "estructuras delictivas cuasi gubernamentales" imponiendo estructuras de gobierno y control sobre la delincuencia y los delincuentes dentro de una localidad y, en algunos casos, corrompiendo a funcionarios públicos (von Lampe, *Organized Crime: Analyzing Illegal Activities*).

[53] Mortley, "A crime of opportunity"; y Akanle, Adesina y Akarah, "Towards human dignity and the internet".

[54] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), "Online scam operations and trafficking into forced criminality in Southeast Asia: recommendations for a human rights response" (Bangkok, Oficina Regional para Asia Sudoriental, 2023); UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Report* (Bangkok, 2023); y *Global Report on Trafficking in Persons 2022* (publicación de las Naciones Unidas, 2022), pág. 102.

[55] Nicholas Ryder y Samantha Bourton, "To exchange or not to exchange – that is the question: a critical analysis of the use of financial intelligence and the exchange of information in the United Kingdom", *Journal of Business Law*, vol. 3 (2024); y Frank S. Perri y Richard G. Brody, "The dark triad: organized crime, terror and fraud", *Journal of Money Laundering Control*, vol. 14, núm. 1 (2011).

[56] Eric Rutger Leukfeldt, "Cybercrime and social ties: phishing in Amsterdam", *Trends in Organized Crime*, vol. 17, núm. 4 (diciembre de 2014); Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime* (Cambridge (Massachusetts, Estados Unidos), Harvard University Press, 2018); y Joshua Oyeniyi Aransiola y Suraj Olalekan Asindemade, "Understanding cybercrime perpetrators and the strategies they employ in Nigeria", *Cyberpsychology, Behavior, and Social Networking*, vol. 14, núm. 12 (diciembre de 2011).

[57] Richet, "How cybercriminal communities grow and change"; Lilian Ablon, Martin C. Libicki y Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Mónica (California, Estados Unidos), RAND Corporation, 2014); y Michael Yip, Nigel Shadbolt y Craig Webber, "Structural analysis of online criminal social networks", en *2012 IEEE International Conference on Intelligence and Security Informatics*, Daniel Zeng *et al.*, eds. (2012).

[58] Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[59] Liu *et al.*, "Understanding, measuring, and detecting"; Shover, Coffey y Sanders, "Dialing for dollars"; y May y Bhardwa, *Organised Crime Groups Involved in Fraud*.

[60] Jay S. Albanese, "Fraud: the characteristic crime of the twenty-first century", *Trends in Organized Crime*, vol. 8, núm. 4 (junio de 2005); Mark Button y Cassandra Cross, *Cyber Frauds, Scams and Their Victims* (Abingdon (Oxon, Reino Unido) y Nueva York, Routledge, 2017); y Robert B. Fried, "Cyber scam artists: a new kind of .con" (2001).

[61] Geralda Odinot *et al.*, *Organised Cybercrime in the Netherlands: Empirical Findings and Implications for Law Enforcement* (La Haya, Centro de Investigación y Datos, Ministerio de Seguridad y Justicia, 2017); Ablon, Libicki y Golay, *Markets for Cybercrime Tools and Stolen Data*; y Michael Yip, Craig Webber y Nigel Shadbolt, "Trust among cybercriminals? Carding forums, uncertainty and implications for policing", *Policing and Society: An International Journal of Research and Policy*, vol. 23, núm. 4 (2013).

de ello es el modelo de delincuencia como servicio[62], en el que los delincuentes realizan intercambios en línea a corto plazo con otros usuarios de Internet que pueden proporcionarles los recursos técnicos necesarios para perpetrar el fraude[63]. Algunos grupos delictivos organizados dedicados al ciberfraude se forman a partir de relaciones que existen íntegramente en línea (p. ej., foros en línea)[64], otros se forman fuera de línea y algunos incorporan a codelincuentes tanto en línea como fuera de línea[65].

Existen grupos delictivos organizados dedicados al fraude de cuello blanco o empresarial que surgen en el seno de organizaciones empresariales legítimas[66]. El abuso de una función legítima para obtener un beneficio ilícito puede servir a los intereses de determinados integrantes de la organización o puede tener por objeto beneficiar a toda la organización[67]. Los grupos delictivos organizados pueden surgir de las estructuras que ya existen en las empresas para llevar a cabo su actividad empresarial legítima, como las funciones y la jerarquía internas de la organización o las relaciones entre distintas empresas. Algunos ejemplos son la implicación de funcionarios de categoría superior y subordinados dentro de la empresa, el recurso a profesionales clave como contadores o abogados, y la comisión conjunta de delitos por parte de distintas organizaciones de un sector, como en los casos de operaciones basadas en información privilegiada[68].

Existen solapamientos entre los distintos tipos de grupos delictivos organizados que se dedican al fraude, en parte debido a la fluidez de los acuerdos de coautoría en determinados entornos en línea y empresariales[69]. Por ejemplo, los ciberempresarios, o los especialistas en finanzas aportan conocimientos especializados y recursos muy valorados por múltiples grupos delictivos organizados que buscan aumentar sus capacidades[70]. La naturaleza fluida y efímera de la coautoría que caracteriza a gran parte del fraude organizado significa que muchos grupos delictivos organizados implicados en él no poseen las estructuras tradicionales observadas en los grupos implicados en otras formas de delincuencia organizada[71]. En consecuencia, es difícil detectar y evaluar grupos poco estructurados y transitorios

[62] Los mercados en línea, los sitios web personalizados y los foros pueden funcionar con su propia estructura organizativa: los administradores, que gestionan los sitios; los moderadores, que regulan el comportamiento en el sitio; los vendedores, que suministran los productos, servicios y conocimientos; y los compradores, que realizan las compras y participan en el intercambio de información. En este contexto, los conocimientos técnicos y los recursos se valoran más que la presencia física y el poder (Yip, Webber y Shadbolt, "Trust among cybercriminals?"; Ildiko Pete *et al.*, "A social network analysis and comparison of six dark web forums", en *5th IEEE European Symposium on Security and Privacy Workshops* (2020); y Choo y Smith, "Criminal exploitation of online systems").

[63] Véanse también Ugur Akyazi, Michael van Eeten y Carlos H. Gañán, "Measuring cybercrime as a service (CaaS) offerings in a cybercrime forum" (Delft (Reino de los Países Bajos), Universidad Tecnológica de Delft, 2021); y Jungkook An y Hee-Woong Kim, "A data analytics approach to the cybercrime underground economy", *IEEE Access*, vol. 6 (2018).

[64] Melvin R. J. Soudijn y Birgit C. H. T. Zegers, "Cybercrime and virtual offender convergence settings", *Trends in Organized Crime*, vol. 15, núms. 2 y 3 (septiembre de 2012).

[65] Leukfeldt, Lavorgna y Kleemans, "Organised cybercrime or cybercrime that is organized?"; y E. Rutger Leukfeldt, Edward R. Kleemans y Wouter P. Stol, "Origin, growth and criminal capabilities of cybercriminal networks: an international empirical analysis", *Crime Law and Social Change*, vol. 67, núm. 1 (febrero de 2017).

[66] Alan Wright, *Organised Crime* (Cullompton (Reino Unido), Willan Publishing, 2006); Gary Slapper y Steve Tombs, *Corporate Crime* (Harlow (Reino Unido), Pearson, 1999); Albanese, "Organized crime as financial crime"; y Michael Levi y Mike Maguire, "Financial and organised crime in Europe: converging paradigms of control?", en *Universalis. Liber amicorum Cyrille Fijnaut*, Toine Spapens, Marc Groenhuijsen y Tijs Kooijmans, eds. (Amberes (Bélgica), Intersentia, 2011).

[67] Por ejemplo, los grupos delictivos corporativos se definieron como una manifestación clave de la delincuencia organizada en el contexto del comercio ilegal de flora y fauna silvestres: los actos delictivos corporativos podrían ser el producto de una toma de decisiones deliberada o de una negligencia culpable dentro de una organización legítima (Tanya Wyatt, Daan van Uhm y Angus Nurse, "Differentiating criminal networks in the wildlife trade: organized, corporate and disorganized crime", *Trends in Organized Crime*, vol. 23, núm. 4 (diciembre de 2020). Véase también Reurink, *Financial Fraud*).

[68] Levi, "Organized fraud and organizing frauds"; y Ruben Herrera *et al.*, "The manipulation of Euribor: an analysis with machine learning classification techniques", *Technological Forecasting and Social Change*, vol. 176, art. núm. 121466 (marzo de 2022).

[69] Leukfeldt, Kleemans y Stol, "Origin, growth and criminal capabilities of cybercriminal networks"; y Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[70] Button y Cross, *Cyber Frauds, Scams and Their Victims*.

[71] Di Nicola, "Towards digital organized crime"; Anita Lavorgna y Anna Sergi, "Serious, therefore organised? A critique of the emerging 'cyber-organised crime' rhetoric in the United Kingdom", *International Journal of Cyber Criminology*, vol. 10, núm. 2 (julio/diciembre de 2016); David S. Wall, "Dis-organised crime: towards a distributed model of the organisation of cybercrime", *European Review of Organised Crime*, vol. 2, núm. 2 (2015); Leukfeldt, Lavorgna y Kleemans, "Organised cybercrime or cybercrime that is organized?"; y Levi, "Organized fraud and organizing frauds".

y responder a ellos. Por ejemplo, en los mercados (o ecosistemas) delictivos en línea, puede resultar difícil saber dónde acaba un grupo delictivo organizado y dónde empieza el siguiente[72]. No obstante, es importante poder reconocer a los grupos delictivos organizados que adoptan estas estructuras diversas para dirigir las medidas contra los delincuentes que tienen mayor impacto.

Es importante señalar que no todos los grupos de delincuentes que cometen fraude constituyen grupos delictivos organizados de conformidad con la definición de la Convención contra la Delincuencia Organizada. Esto se debe a que la comisión de fraudes graves es también un principio clave que define a la delincuencia organizada. Las características fundamentales de un delito grave en el contexto de los actos de fraude se analizarán en la sección siguiente.

ESTUDIO DE CASO: FRAUDE DEL APOYO TÉCNICO

Los autores del fraude del apoyo técnico desarrollaron sitios web fraudulentos que imitaban servicios legítimos de este tipo (p. ej., de *software* de seguridad o reparación de impresoras), que se anunciaban utilizando motores de búsqueda de Internet convencionales. A quienes visitaban el sitio web se les pedía que llamaran a un número de teléfono, tras lo cual la persona que atendía la llamada convencía a la víctima para que pagara importantes cantidades de dinero por un servicio falso o innecesario. Los delincuentes implicados en estas estafas operaban en el marco de una vibrante economía informal, en la que grupos delictivos organizados compraban y vendían servicios especializados en grupos de chat que funcionaban en plataformas de medios sociales convencionales. Los delincuentes operaban como subempresas discretas que cumplían funciones específicas en la comisión del fraude del apoyo técnico. Estas funciones incluían a los operadores de los centros de llamadas que atendían las llamadas de las víctimas, a los grupos especializados en blanqueo de dinero que vendían sus servicios a los centros de llamadas y a las personas que armaban y promocionaban los sitios web y vendían y redirigían las llamadas de las víctimas a los operadores de los centros de llamadas. Aunque gran parte de la colaboración entre las distintas subempresas se llevaba a cabo en línea, muchos de los delincuentes se encontraban en la India. Gran parte de los centros de llamadas operaban desde oficinas situadas en grandes ciudades de la India y se publicaban regularmente en los foros en línea anuncios de trabajo para agentes de llamadas en los que se ofrecían detalles sobre el sueldo y las prestaciones laborales.

Fuente: Jienan Liu *et al.*, "Understanding, measuring, and detecting modern technical support scams", en *8th Institute of Electrical and Electronics Engineers (IEEE) European Symposium on Security and Privacy*, ponencia presentada en el simposio celebrado en Delft (Reino de los Países Bajos), del 3 al 7 de julio de 2023.

[72] Por ejemplo, véase Erika Kraemer-Mbula, Puay Tang y Howard Rush, "The cybercrime ecosystem: online innovation in the shadows?", *Technological Forecasting and Social Change*, vol. 80, núm. 3 (marzo de 2013).

ESTUDIO DE CASO: FRAUDE AL CONSUMIDOR

Un delincuente creó varias tiendas en línea falsas que parecían creíbles, por ser similares a las de minoristas convencionales en línea, aunque ninguno de los productos anunciados en el sitio existía. Los sitios web se anunciaban profusamente en un motor de búsqueda de Internet convencional, en sitios web de comparación de precios y en periódicos. Cada cliente que realizaba un pedido recibía automáticamente una confirmación, un recibo y una solicitud de pago por transferencia electrónica. El delincuente buscó un cómplice que lo ayudara a suministrar las cuentas bancarias para recibir el dinero y lo encontró en un foro de la red oscura. Este coautor lo asesoró sobre la manera de blanquear el producto del delito y evitar ser detectado por las autoridades. Ayudó a reclutar múltiples mulas de dinero con cuentas bancarias en el extranjero que acordaron recibir los pagos de los clientes, quedándose con el 15 por ciento y enviando el resto a los dos delincuentes principales, que se repartirían el resto de los beneficios del delito. El grupo consiguió robar más de 280.000 euros a los clientes.

Fuente: Tribunal de Distrito de Múnich, sentencia, 7 de junio de 2017 (LG München, Urteil vom 07.06.2017, 19 KLs 30 Js 18/15), disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

ESTUDIO DE CASO: FRAUDE EN SUBASTAS CON PARTICIPACIÓN DE UN GRUPO DELICTIVO ORGANIZADO HÍBRIDO, CON INTEGRANTES EN LÍNEA Y FUERA DE LÍNEA

Los delincuentes perpetraban fraudes en línea en los que se anunciaban artículos inexistentes a consumidores de los Estados Unidos de América en sitios de subastas convencionales. Todos los miembros del grupo que planearon y prepararon el plan fraudulento se encontraban en la misma ciudad de Rumanía. Pedían a los consumidores que realizaran los pagos con tarjetas de débito prepagadas. Estos pagos eran cobrados por otros asociados y terceros que blanqueaban el dinero y se encontraban en los Estados Unidos. Una vez cobrados los pagos de las víctimas, los delincuentes radicados en los Estados Unidos convertían el dinero en bitcoines, que se transferían al grupo de Rumanía. Se utilizaban intercambiadores de bitcóin para convertir el dinero en la moneda local, entre ellos uno operado por un ciudadano búlgaro cómplice de facilitar el proceso de blanqueo de dinero.

Fuente: *United States of America v. Andre-Catalin Stoica et al.*, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

Delitos graves en el contexto del fraude

El concepto de delito grave ocupa un lugar central en la definición del ámbito de aplicación de la Convención contra la Delincuencia Organizada. Para que la Convención sea aplicable, el delito cometido por el grupo delictivo organizado debe cumplir los criterios definidos (incluida la transnacionalidad y la participación de un grupo delictivo organizado) y ser punible con una privación de libertad máxima de al menos cuatro años en la legislación interna. Por lo tanto, el uso de la noción de delito grave con referencia a la legislación nacional de los Estados proporciona suficiente flexibilidad para que la Convención se aplique a una amplia gama de manifestaciones de la delincuencia organizada transnacional, incluido el fraude.

En el artículo 2 b) de la Convención se define "delito grave" como "la conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave". En el artículo 3, párrafo 2, de la Convención se definen los criterios para determinar, a los efectos de la aplicación de la Convención, cuándo se considerará que un delito tiene carácter transnacional.

A escala internacional, los ordenamientos jurídicos existentes son equívocos en cuanto a la gravedad del fraude. Los factores agravantes específicos que pueden agravar individual o acumulativamente las penas para las personas condenadas por fraude, y la pena máxima que puede aplicarse en un caso de fraude, difieren en las distintas jurisdicciones legales (véase el cap. V). Esto se refleja en las penas impuestas a quienes cometen delitos de fraude: por ejemplo, se ha demostrado que las penas privativas de libertad de larga duración impuestas a los delincuentes de cuello blanco que defraudan a instituciones son escasas, a pesar de la prevalencia de este delito y de los elevados beneficios que obtienen los delincuentes[73]. Además, algunos de los tipos de fraude más sofisticados rozan las líneas difuminadas que separan las prácticas legítimas de las ilegítimas, y el derecho penal (y su aplicación) puede ser sustituido por las leyes civiles aplicadas por los organismos reguladores del sector público en general[74]. El tratamiento desigual del fraude en la legislación fomenta la ambigüedad a la hora de identificar los casos de fraude "grave" y a quienes lo cometen.

Hay que tener en cuenta dos dimensiones principales de la gravedad[75]:

- El perjuicio que puede atribuirse al fraude, ya sea en términos de la víctima o grupo de víctimas identificable o del impacto más amplio que tiene en las instituciones legítimas[76]
- La culpabilidad moral del autor o los autores, es decir, hasta qué punto determinadas conductas violan las normas morales aceptadas en la sociedad[77]

Las distintas víctimas, experiencias de las víctimas, conductas delictivas y métodos hacen que, como categoría delictiva, el fraude incorpore una criminalidad muy diversa en relación con la gravedad de los perjuicios causados y la ilicitud moral de las conductas delictivas. Son múltiples los factores que puede considerarse que agravan un delito de fraude, entre ellos el impacto financiero y el daño a la víctima, pero también conductas delictivas específicas como dirigirse a víctimas vulnerables, tener contacto repetido con la misma víctima para utilizar métodos más complejos o insidiosos (p. ej., la seducción), abusar de una posición de confianza o autoridad para defraudar a las víctimas y apuntar a un gran número de víctimas[78].

Es necesario considerar las pruebas sobre las características de los delitos de fraude que pueden utilizarse para determinar si ciertos delitos de fraude deben tratarse como delitos graves en términos de imposición de penas y de política de justicia penal en general. Esas características se exponen en las secciones siguientes.

---

[73] Michael Levi, "Hitting the suite spot: sentencing frauds", *Journal of Financial Crime*, vol. 17, núm. 1 (2010); y Lisa Marriott, "White-collar crime: the privileging of serious financial fraud in New Zealand", *Social and Legal Studies*, vol. 29, núm. 4 (agosto de 2020).

[74] Button y Cross, *Cyber Frauds, Scams and Their Victims*.

[75] An Adriaenssen *et al.*, "Public perceptions of the seriousness of crime: weighing the harm and the wrong", *European Journal of Criminology*, vol. 17, núm. 2 (marzo de 2020); Jonas Visschers y Letizia Paoli, "A comparison of public and police perceptions of the seriousness of crime", *European Journal on Criminal Policy and Research* (2024); y Victoria A. Greenfield y Letizia Paoli, "A framework to assess the harms of crimes", *The British Journal of Criminology*, vol. 53, núm. 5 (septiembre de 2013).

[76] Tom Sorell, "The scope of serious crime and preventive justice", *Criminal Justice Ethics*, vol. 35, núm. 3 (2016).

[77] Por ejemplo, independientemente del daño que se experimente, el robo con allanamiento de morada podría interpretarse como una mayor violación de las normas morales que el hurto, debido al ataque a la integridad del hogar de la víctima.

[78] Button *et al.*, "Online frauds".

Pérdidas e impacto en el ámbito financiero

El fraude es un delito adquisitivo y el valor del dinero robado (o que se pretendía robar) sirve para determinar su gravedad. Puede considerarse como la suma de las pérdidas previstas o reales atribuibles a los delincuentes que defraudan a múltiples víctimas. Las distintas conductas delictivas pueden dar lugar a modalidades diferenciadas de fraude y pérdidas financieras. Algunas tramas fraudulentas afectan a un número relativamente pequeño de víctimas que pierden sumas importantes de dinero[79], mientras que otras defraudan a un mayor número de víctimas en montos menores[80]. La evaluación de las pérdidas sufridas por las víctimas también puede tener en cuenta quiénes son las víctimas (p. ej., una persona física o jurídica), la proporción del patrimonio de la víctima que se ha perdido a causa del fraude y otros daños colaterales más amplios causados[81]. El fraude puede socavar sectores legítimos, imponiendo costos que van más allá de las pérdidas directas a la organización víctima[82].

Daños a las víctimas

La mayoría de los casos de fraude se producen a puerta cerrada y rara vez implican delitos visibles o viscerales, como la violencia grave en que suelen centrarse los organismos encargados de hacer cumplir la ley. Además, las políticas de imposición de penas de la justicia penal pueden centrarse exclusivamente en las pérdidas económicas, sin tener en cuenta el impacto del fraude en las personas. La investigación ha identificado víctimas que experimentan un considerable efecto perjudicial en su bienestar psicológico y emocional y en su salud física; en casos extremos, las víctimas se han quitado la vida como consecuencia del fraude[83]. Las respuestas de las víctimas son muy subjetivas y pueden estar determinadas por sus circunstancias personales y las particularidades de la metodología del fraude[84]. La naturaleza diversa y subjetiva de las experiencias de las víctimas significa que hay dificultades para determinar la vulnerabilidad y el perjuicio causado al gran número de víctimas de fraude[85].

Culpabilidad del autor del fraude

La culpabilidad refleja en parte el nivel de intención delictiva que muestra el autor de un acto, como el grado de planificación y premeditación y las pruebas de reincidencia. Los complejos procesos que se siguen para perpetrar un fraude suelen conllevar fases de planificación y preparación, y algunos delincuentes aplican continuamente nuevos métodos para aprovechar el amplio abanico de oportunidades

---

[79] Por ejemplo, véase Skidmore, *Protecting People's Pensions.*

[80] Por ejemplo, véase Marguerite DeLiema y Paul Witt, *Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam*, documento de trabajo, núm. 2021-434 (Ann Arbor (Estados Unidos), Universidad de Michigan, Michigan Retirement and Disability Research Center, 2021).

[81] Michael Levi, "Organized fraud" en *The Oxford Handbook of Organized Crime*, Letizia Paoli, ed. (Oxford (Reino Unido), Oxford University Press, 2014); y Xin Qingquan, Jing Zhou y Fang Hu, "The economic consequences of financial fraud: evidence from the product market in China", *China Journal of Accounting Studies*, vol. 6, núm. 1 (2018).

[82] Por ejemplo, el denominado fraude de choque por dinero, dirigido contra el sector de los seguros de automóviles, puede elevar las primas de seguro para el público (David S. Wall, Yulia Chistyakova y Stefano Bonino, "Crash-for-cash and VAT carousels: organised crime infiltration in the United Kingdom", en *Organised Crime in European Businesses*, Ernesto Savona, Michele Riccardi y Giulia Berlusconi, eds. (Londres, Routledge, 2016)).

[83] Por ejemplo, véanse Button, Lewis y Tapley, "Not a victimless crime"; Cassandra Cross, "(Mis)understanding the impact of online fraud: implications for victim assistance schemes", *Victims and Offenders*, vol. 13, núm. 6 (2018); Raoul Notté *et al.*, "Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands", *International Review of Victimology*, vol. 27, núm. 3 (septiembre de 2021); y Encarnación Sarriá *et al.*, "Financial fraud, mental health, and quality of life: a study on the population of the city of Madrid, Spain", *International Journal of Environmental Research and Public Health*, vol. 16, núm. 18 (septiembre de 2019).

[84] Por ejemplo, se ha demostrado que el fraude romántico causa un gran malestar psíquico a las víctimas (Tom Buchanan y Monica T. Whitty, "The online dating romance scam: causes and consequences of victimhood", *Psychology, Crime and Law*, vol. 20, núm. 3 (2014). Véase también Katelyn A. Golladay y Jamie A. Snyder, "Financial fraud victimization: an examination of distress and financial complications", *Journal of Financial Crime*, vol. 30, núm. 6 (2023)).

[85] Michael Skidmore, Janice Goldstraw-White y Martin Gil, "Vulnerability as a driver of the police response to fraud", *Journal of Criminological Research, Policy and Practice*, vol. 6, núm. 1 (2020); y Sara Correia, "Cybercrime victims: victim policy through a vulnerability lens", Social Science Research Network Working Paper (2021). En el Reino Unido se presta cada vez más atención a la identificación de las víctimas vulnerables, en particular las que corren el riesgo de ser objeto de ataques reiterados.

disponibles para delinquir[86]. El crecimiento de las tecnologías de la información y las comunicaciones ha "industrializado" los delitos de fraude, ofreciendo a los delincuentes mayores posibilidades de cometerlos a una escala sin precedentes, con rapidez y a bajo costo[87]. Los delincuentes pueden aprovechar la tecnología para atacar a muchas víctimas simultáneamente, en algunos casos mediante la automatización[88]. Además, las tecnologías de la información y las comunicaciones están globalizadas por defecto y, en algunos casos, hay poca diferencia práctica entre perpetrar un fraude de nivel local y uno transnacional[89]. En este contexto, puede ser difícil diferenciar a los delincuentes que cometen delitos graves de los que no lo hacen.

Los métodos específicos empleados para captar y defraudar a las víctimas pueden determinar la gravedad percibida de las acciones del autor del delito. Esto incluye dirigirse, a veces repetidamente, a personas que de alguna manera están en desventaja, como víctimas que se perciben como vulnerables (p. ej., personas con discapacidad)[90]. El abuso de una posición de poder o confianza también se considera un factor agravante en los delitos de fraude en algunas jurisdicciones legales[91]. Por último, la implicación de un grupo delictivo organizado puede multiplicar por sí misma los efectos adversos del fraude y constituir un indicio de una intención delictiva y culpabilidad mayores. Un grupo delictivo organizado que mantiene una "institución" delictiva con un suministro constante de coautores para perpetrar fraudes de forma continuada (así como otros delitos secundarios, como la piratería informática ilícita y el blanqueo de dinero)[92] puede incurrir en un delito considerado más grave[93]. Además, el delito puede agravarse aún más cuando el grupo es capaz de desafiar o socavar la autoridad y los sistemas del Estado y los sectores legítimos (p. ej., mediante la corrupción)[94].

Los marcos de imposición de penas en el sistema de justicia penal proporcionan una orientación importante a los organismos encargados de hacer cumplir la ley a la hora de decidir a dónde destinar los recursos disponibles. El aumento del alcance y la complejidad de los delitos de fraude, en particular los que son posibles gracias a la tecnología, plantea retos a la hora de detectar casos graves de fraude, pero se necesitan marcos sólidos para afrontar los casos de fraude más atroces. Las dimensiones precisas del fraude organizado en cada Estado Miembro deberán tenerse en cuenta en las decisiones sobre políticas relativas a la dotación de recursos a las fuerzas de seguridad y en las estrategias más amplias de prevención de la delincuencia para hacer frente al fraude. Históricamente, sin embargo, no se ha concedido al fraude cometido por grupos delictivos organizados el mismo grado de prioridad que a

---

[86] Por ejemplo, véanse Kraemer-Mbula, Tang y Rush, "The cybercrime ecosystem"; y Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[87] Button y Cross, *Cyber Frauds, Scams and Their Victims*; y Michael Levi *et al.*, *The Implications of Economic Cybercrime for Policing, Research Report* (Londres, City of London Corporation, 2015).

[88] Wall, "Dis-organised crime"; y van der Wagen y Pieters, "From cybercrime to cyborg crime".

[89] Levi *et al.*, *The Implications of Economic Cybercrime for Policing.*

[90] Las investigaciones sobre las opiniones del público en el Reino Unido mostraron que los métodos insidiosos, como la captación financiera, se percibían como tipos de fraude más graves (véase Jane Kerr *et al.*, *Research on Sentencing Online Fraud Offences* (Londres, Sentencing Council, 2013)).

[91] Marriott, "White-collar crime"; véase también el capítulo V del presente documento temático.

[92] Leukfeldt y Jansen, "Cyber criminal networks and money mules"; Jonathan Lusthaus *et al.*, "Cybercriminal networks in the United Kingdom and beyond: network structure, criminal cooperation and external interactions", *Trends in Organized Crime* (2023); David S. Wall, "Digital realism and the governance of spam as cybercrime", *European Journal on Criminal Policy and Research*, vol. 10, núm. 4 (diciembre de 2004); y Michael Yip, Nigel Shadbolt y Craig Webber, "Why forums? An empirical analysis into the facilitating factors of carding forums", en *Proceedings of the 3rd Annual ACM Web Science Conference* (París, 2013).

[93] Sorell, "The scope of serious crime".

[94] Por ejemplo, los grupos delictivos organizados que operan en toda Asia Sudoriental se dedican a la delincuencia sistémica y obtienen beneficios del fraude estimados en miles de millones de dólares. Estos grupos están implicados desde hace tiempo en diversas formas de delincuencia organizada, y la capacidad de cometer fraudes a esta escala está vinculada a la evolución paralela de la banca clandestina y el blanqueo de dinero, concretamente en los casinos. Los casinos pueden facilitar el blanqueo de dinero, pero también servir de tapadera y dar facilidades para emplear a una amplia mano de obra que coopere en la comisión de delitos desde recintos donde se cometen las estafas. Además, algunos grupos operan a propósito desde países en los que la gobernanza y el estado de derecho son débiles y los funcionarios públicos son susceptibles de corrupción (véase ACNUDH, "Online scam operations and trafficking into forced criminality in Southeast Asia"; y UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*, Technical Policy Brief (Bangkok, 2024)).

otras manifestaciones de la delincuencia organizada[95] y a menudo el fraude organizado se ha percibido como una actividad complementaria de los grupos delictivos organizados implicados en otros delitos más graves (p. ej., el tráfico de drogas)[96].

Interseccionalidad

Un concepto clave para comprender las experiencias de las personas con el fraude organizado es la interseccionalidad. La interseccionalidad constituye un marco para analizar cómo se entrecruzan el poder y la identidad al influir en las relaciones sociales y las experiencias individuales. Pone de relieve que las experiencias de hombres, mujeres y personas de género diverso interactúan con su clase, raza, edad, etnia e identidad sexual y otras identidades, configurando así las formas en que las personas son percibidas en la sociedad. En el contexto del fraude organizado, un análisis interseccional es una herramienta útil para comprender las diferentes tendencias y motores para participar en el fraude organizado y convertirse en víctima de él. Esto no quiere decir que determinadas características de identidad lleven a una persona a ser intrínsecamente vulnerable al fraude organizado, sino que, debido a factores estructurales, históricos y contextuales, el privilegio y el poder de una persona pueden verse afectados en circunstancias específicas, dando lugar a experiencias diferenciadas de fraude organizado. El estudio de caso que figura a continuación muestra cómo los grupos delictivos organizados pueden aprovecharse de la exclusión social e histórica a la que se enfrentan las personas con discapacidad para llevar a cabo actos de fraude organizado.

ESTUDIO DE CASO: PRODUCTOS Y SERVICIOS DE CONSUMO Y FRAUDE EN LAS INVERSIONES

En el Reino Unido, un pequeño grupo delictivo organizado familiar realizó durante varios años tareas para captar como víctima a una persona que padecía una enfermedad neurológica progresiva. El delincuente principal era aparentemente un comerciante que conoció a la víctima cuando buscaba clientes potenciales. El grupo realizó y cobró en exceso multitud de reparaciones y trabajos de mantenimiento de baja calidad en la casa de la víctima. Además, la convencieron para que les entregara 240.000 libras, que incluían dinero para una supuesta oportunidad de inversión. La víctima no reconoció su condición de tal porque los autores se habían esforzado mucho por entablar con él una relación de amistad y, en consecuencia, pensó que estaba ayudando a sus amigos. El fraude fue finalmente denunciado por su cuidador y los agentes del orden tuvieron que explicarle detenidamente cómo y por qué había sido víctima de un fraude. Este ejemplo ilustra la manera en que algunos grupos delictivos organizados tienen como objetivo a las personas con discapacidad debido a la probabilidad de que estas personas experimenten aislamiento social y no tengan un acceso adecuado a apoyo social.

Fuente: Coretta Phillips, "From 'rogue traders' to organized crime groups: doorstep fraud of old-er adults", *The British Journal of Criminology*, vol. 57, núm. 3 (mayo de 2017).

[95] Alan Doig y Michael Levi, "A case of arrested development? Delivering the UK National Fraud Strategy within competing policing policy priorities", *Public Money and Management*, vol. 33, núm. 2 (2013); y Cassandra Cross y Dom Blackshaw, "Improving the police response to online fraud", *Policing*, vol. 9, núm. 2 (junio de 2015).

[96] Levi, "Organized fraud", en *The Oxford Handbook of Organized Crime*.

Es importante reconocer que no existen rasgos de identidad específicos que hagan a una persona más vulnerable al fraude organizado. Esto se debe a sus múltiples manifestaciones y tipologías. Por ejemplo, una persona con ingresos elevados puede ser objeto de fraude en las inversiones, mientras que una persona de un nivel socioeconómico más bajo puede ser objeto de fraude relacionado con el empleo. Por este motivo, y para poder desarrollar medidas preventivas eficaces, es importante recopilar datos interseccionales y desglosados por género y realizar análisis para determinar por qué determinadas poblaciones pueden ser objeto de distintos tipos de fraude.

--

CAPÍTULO II

Categorías de fraude organizado

Los delitos de fraude son muy diversos, en cuanto a los métodos empleados, las entidades contra las que van dirigidos y el impacto en las víctimas y en los sistemas en general. Este documento temático se centra en el fraude organizado dirigido contra particulares o instituciones privadas con el fin de obtener un beneficio económico u otro beneficio de orden material.

Las categorías de la tipología se ordenan según las narrativas o artimañas generales y dominantes que se presentan a las víctimas del fraude[97]; por ejemplo, el anuncio de una oportunidad laboral en el fraude relacionado con el empleo. Sin embargo, también se incluye la categoría de fraude contra empresas y organizaciones para abarcar toda la gama de fraudes contra ese tipo de entidades[98], incluido el abuso de los sistemas por parte de autores internos o externos a la organización[99]. De este modo, las categorías de fraude se ordenan principalmente en función de una perspectiva del fraude basada en la víctima, y no en los procesos subyacentes en la comisión del delito, como los procesos de robo de datos personales o los modos de comercialización u otras formas de comunicación masiva.

Las categorías clave que se describirán en las siguientes secciones del documento temático son:

[97] Véase, por ejemplo, Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud".

[98] Esta categoría se incluyó para garantizar el reconocimiento de las empresas y organizaciones como grupo clave de víctimas. Otras categorías, como el fraude en productos y servicios de consumo y la suplantación de identidad, también pueden provocar pérdidas financieras a empresas y organizaciones.

[99] Véase la introducción del presente documento temático para un análisis más detallado de la elaboración de la tipología.

Al ordenar las categorías en función de las distintas narrativas o artimañas presentadas a las víctimas, esta tipología pone de manifiesto otras amplias distinciones en las técnicas utilizadas para manipular a las víctimas para que se desprendan de su dinero. Entre las principales distinciones figuran el uso de ventas y alicientes en productos y servicios de consumo, el fraude relacionado con el empleo y el fraude en las inversiones de consumidores; el miedo y la autoridad que caracterizan a muchos tipos de fraude en los que el autor se hace pasar por una persona u organización fiable; la manipulación de información y sistemas comerciales y financieros en la falsificación de identidad, y la captación financiera y la explotación en el fraude basado en las relaciones y la confianza. Otros elementos de la interacción con los delincuentes que pueden afectar a la experiencia de las víctimas (p. ej., la forma de establecer contacto o el período de tiempo durante el que son objeto de los delincuentes) se tratarán cuando sea pertinente en cada categoría.

Las categorías descritas en la presente sección no pretenden ser exhaustivas, debido a la gama casi ilimitada de metodologías que pueden emplear los delincuentes, que se adaptan continuamente a los nuevos contextos socioeconómicos, sistemas y tecnología. Cada categoría general se complementa con subcategorías destacadas que se describen en cada sección. No todas las categorías de fraude son perpetradas exclusivamente por grupos delictivos organizados, pero el debate se centrará en el fraude organizado.

La línea que separa el fraude de las conductas que no constituyen delito puede ser delgada. Por ejemplo, no todos los casos en que un producto o servicio no se ajusta a lo que se anuncia y vende a un consumidor cumplen los criterios jurídicos de fraude; de acuerdo con lo expuesto en el capítulo I, dependerá de si hubo intención delictiva de engañar al comprador. En el contexto de la delincuencia organizada, la intención delictiva es evidente en muchas acciones clave, como la planificación y las fases preparatorias para poner en práctica un engaño y la utilización de la técnica de engaño contra múltiples víctimas. Se supone que todas las categorías y casos analizados en la presente sección cumplen la definición de fraude expuesta en el capítulo I: quienes los cometen son penalmente responsables debido a un uso deliberado del engaño con el fin de obtener un beneficio financiero u otro beneficio de orden material.

Fraude en productos y servicios de consumo

El fraude en productos y servicios de consumo es un tipo frecuente de fraude, y son muchas las personas que denuncian haber sido estafadas, haber sido objeto de él o haberse visto expuestas a comunicaciones de venta de productos o servicios fraudulentos[100]. A menudo, quienes cometen este tipo de fraudes comercializan productos de gran demanda u ofrecen productos y servicios a un costo inferior al del mercado legítimo. El fraude de productos y servicios al consumidor implica la venta de productos o servicios inexistentes o que difieren significativamente de lo que se anuncia (incluida mercancía falsificada vendida como auténtica)[101]. El fraude por falta de entrega consiste en anunciar y cobrar productos o servicios totalmente ficticios o que el autor del fraude no tiene intención de suministrar[102]. Quienes realizan la venta engañosa de productos y servicios distorsionan los datos de los bienes o servicios que suministran. Puede ser difícil confirmar la existencia de un fraude cuando el producto o servicio se recibe pero se considera que no corresponde a lo anunciado y es necesario determinar de qué manera y hasta

[100] Por ejemplo, el fraude por impago o falta de entrega es uno de los ciberdelitos más frecuentemente denunciados en los Estados Unidos (Estados Unidos, Buró Federal de Investigaciones, "Internet crime report 2023" (2023); véase también Comisión Europea, "Survey on 'scams and fraud experienced by consumers': final report" (Bruselas, 2020)).

[101] Button y Cross, *Cyber Frauds, Scams and Their Victims*; véase también *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (publicación de las Naciones Unidas, 2010), cap. 8.

[102] Estados Unidos, Buró Federal de Investigaciones, "How we can help you: holiday scams", disponible en http:///www.fbi.gov/.

qué punto es distinto de lo publicado o vendido[103]. Algunos delincuentes dirigen sus anuncios a los grupos considerados más susceptibles de ser víctimas de una estafa concreta[104]. A veces, se aprovechan de la falta de conocimientos financieros y técnicos de la víctima para venderle servicios financieros como préstamos, planes de seguros o productos de pensiones[105]. Suelen referirse a productos cuyo valor reside en el futuro, y a las víctimas o bien se les ofrece una previsión excesivamente optimista de los resultados futuros o bien no se les explican adecuadamente los riesgos. También es posible que no se informe a la víctima de los gastos, las comisiones o los requisitos legales, lo que puede acarrear más pérdidas y penalizaciones[106].

Entre los productos y servicios que suelen aparecer en los fraudes en productos y servicios de consumo figuran las piedras preciosas, los animales domésticos, las entradas para eventos, los productos médicos, los alimentos, los seguros, los productos o servicios de clarividencia o psíquicos, los préstamos y el alivio de la deuda[107]. Sin embargo, existe una variedad casi infinita de productos y servicios que pueden utilizarse en las actividades fraudulentas, ya que quienes cometen fraudes tratan de adaptarse continuamente y sacar partido de los nuevos mercados y demandas de los consumidores. Un ejemplo de esto se presentó durante la pandemia de enfermedad por coronavirus (COVID-19), cuando se anunciaban productos médicos falsos o inexistentes[108].

Este aumento de la diversidad se ha visto facilitado por el crecimiento de los sitios comerciales en línea, en particular los sitios de ventas y subastas entre pares, y, cada vez más, las plataformas de medios sociales en las que se venden todo tipo de productos[109]. Los productos y servicios se comercializan a través de diversos medios, como sitios web falsos, sitios legítimos de compras y subastas y correos basura. Otros métodos son el correo postal, la comercialización de gran volumen y las llamadas de ventas de telemercadeo, las ventas a domicilio, los envíos masivos y las llamadas telefónicas no solicitadas[110]. Algunos delincuentes se aprovechan del dinámico mercado de listas de clientes potenciales recopiladas por medios legítimos o ilegítimos (como una violación de datos o una campaña de suplantación de identidad en línea) o incluso de directorios de personas que ya han sido víctimas en el pasado[111]. Las tecnologías de la información y las comunicaciones han aumentado enormemente la capacidad de comercializar y vender productos y servicios a escala mundial y a un costo comparativamente bajo. En algunos casos, es posible que el consumidor pierda dinero, pero dependiendo de las circunstancias y los métodos empleados por los delincuentes, una plataforma de ventas o un proveedor de servicios financieros pueden incurrir también en una pérdida financiera. Entre las metodologías clave cabe citar:

- La creación de sitios web falsos con fines de comercialización o venta de productos y servicios. Los delincuentes pueden anunciar el sitio web utilizando canales digitales, como los medios sociales o el correo electrónico basura, o pueden manipular los motores de búsqueda de Internet

[103] En algunas regiones, los reguladores del sector público pueden ser responsables de identificar el fraude y responder a él. Entre estos reguladores se encuentran los organismos encargados de proteger a los consumidores o regular las prácticas profesionales.

[104] Keith B. Anderson, "Mass-market consumer fraud: who is most susceptible to becoming a victim?", documento de trabajo, núm. 332 (Washington D. C., Oficina de Economía, Comisión Federal de Comercio, 2016). Véase también el debate sobre la comercialización masiva en el capítulo IV del presente documento temático.

[105] El fraude en las inversiones se incluye como una categoría aparte más adelante (véase también Reurink, *Financial Fraud*).

[106] Véase, por ejemplo, Skidmore, *Protecting People's Pensions*.

[107] Las inversiones de los consumidores se incluyen a continuación como una categoría aparte (véase también Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud"; y Mark Button, Chris Lewis y Jacki Tapley, "Fraud typologies and the victims of fraud: literature review" (Londres, National Fraud Authority, 2009)).

[108] Reino Unido, Organismo Nacional de Lucha contra la Delincuencia, "Beware fraud and scams during COVID-19 pandemic fraud", 26 de marzo de 2020.

[109] Emma Fletcher, "Social media: a golden goose for scammers", Comisión Federal de Comercio, 6 de octubre de 2023.

[110] Marguerite DeLiema y Lynn Langton, "Older victims of mass marketing scams: an analysis of data seized from scammers", *Innovation in Aging*, vol. 5, supl. núm. 1 (2021); Coretta Phillips, "From 'rogue traders' to organized crime groups: doorstep fraud of older adults", *The British Journal of Criminology*, vol. 57, núm. 3 (mayo de 2017); y Shover, Coffey y Sanders, "Dialing for dollars".

[111] Levi, "Organized fraud", en *The Oxford Handbook of Organized Crime*, pág. 460; y Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

para aumentar la probabilidad de que quienes buscan productos o servicios determinados lleguen a su sitio web[112].

- La creación de vendedores falsos en plataformas legítimas de venta, subasta o medios sociales que utilizan cuentas abiertas con identidades falsas o robadas. Estos vendedores explotan plataformas legítimas que dan acceso a un gran volumen de usuarios que buscan productos y servicios. Por ejemplo, un grupo delictivo organizado publicó cientos de miles de anuncios de artículos de gran valor, como automóviles, en múltiples sitios de subastas[113].

El fraude al consumidor en línea no tiene por qué ser sofisticado ni complejo. Para aprovechar fraudulentamente un sitio legítimo de ventas o subastas puede bastar con que una persona abra una cuenta en un sitio de subastas y publique un anuncio para vender un producto inexistente. La función de la delincuencia organizada rara vez queda al descubierto en el intercambio con la víctima, sino que se percibe más bien al comprender la planificación y preparación que hay detrás. Por ejemplo, la producción, el transporte, la venta y la distribución de productos falsificados forman parte de un proceso complejo que requiere la participación de grupos delictivos organizados con altos niveles de coordinación entre los coautores[114]. En el contexto del ciberfraude, entre las etapas clave cabe citar el establecimiento y la comercialización del perfil de la plataforma o sitio web, la captación de víctimas para mantener el engaño (o conseguir nuevos pagos) y el movimiento del dinero. Los delincuentes pueden adoptar diversos métodos para recibir los pagos, como convencer a un proveedor de servicios de pago de que su empresa es legítima, desviar a los clientes a sitios de pago falsos, pedir a las víctimas que utilicen tarjetas de débito prepagadas y utilizar cuentas de terceros, ya sea de mulas de dinero o cuentas abiertas con identidades robadas o falsas. Algunos autores de fraudes transnacionales reclutan a coautores dentro del país objetivo para facilitar el blanqueo de dinero[115]. Las cuentas bancarias suelen estar registradas con identidades falsas, robadas o prestadas (p. ej., mulas de dinero), por lo que el rastro financiero es limitado.

ESTUDIO DE CASO: FRAUDE AL CONSUMIDOR EN LAS COMPRAS EN LÍNEA

Un sitio web independiente de venta en línea anunciaba al público bienes de consumo de gran demanda en el Reino Unido de Gran Bretaña e Irlanda del Norte y recibió miles de pedidos de consumidores durante un período de aproximadamente tres meses, la mayoría de los cuales no se cumplieron. El grupo delictivo organizado había adoptado la forma de una cadena de suministro en la que había un delincuente en el extranjero que era, en apariencia, el proveedor de la mercancía, y un centro de distribución y un minorista en línea situados en regiones distintas del Reino Unido. La adopción de la estructura formal de una cadena de suministro daba un barniz de legitimidad que podía utilizarse para engañar al proveedor de servicios de pago a fin de que le diera acceso a su servicio de pago en línea para tomar los pedidos de los clientes. La mayoría de los productos que se vendían nunca habían existido y el dinero de las compras se transfería al proveedor ficticio en el extranjero y se retiraba en efectivo.

Fuente: Michael Skidmore y Beth Aitkenhead, "Understanding the characteristics of serious fraud offending in the UK" (Londres, The Police Foundation, 2023).

[112] Quien comete el fraude puede pagar a la empresa tecnológica o perpetrar un "fraude de clics", mediante el cual se utilizan bots para repetir clics en el enlace de un sitio web con el fin de inflar su clasificación en las búsquedas, haciendo así que el sitio parezca más legítimo.

[113] Véase *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

[114] Hulme, Disley y Blondes, eds., *Mapping the Risk of Serious and Organised Crime*.

[115] Christine Conradt, "Online auction fraud and criminological theories: the Adrian Ghighina case", *International Journal of Cyber Criminology*, vol. 6, núm. 1 (2012); y Jack M. Whittaker y Mark Button, "Understanding pet scams: a case study of advance fee and non-delivery fraud using victims' accounts", *Journal of Criminology*, vol. 53, núm. 4 (diciembre de 2020).

ESTUDIO DE CASO: FRAUDE AL CONSUMIDOR EN LAS SUBASTAS EN LÍNEA

Un grupo delictivo organizado publicó anuncios de productos de valor alto en varios sitios web de subastas en línea. Los archivos de imagen que se publicaban en cada anuncio contenían un programa malicioso que infectaba el dispositivo del cliente cuando este hacía clic en ellos. El objetivo del programa malicioso era redirigir imperceptiblemente a los clientes a páginas web falsificadas que parecían idénticas a las del sitio web legítimo. Las páginas web incluían una función de chat en directo que permitía al comprador hablar con agentes del servicio de atención al cliente que eran codelincuentes del grupo. Se pedía a los clientes que pagaran los artículos a través de un "agente de garantía", que presuntamente retenía el dinero para el comprador hasta que este confirmaba la recepción del artículo. Sin embargo, el dinero se ingresaba en cuentas controladas por los delincuentes y las víctimas no recibían ni los artículos encargados ni un reembolso.

Fuente: United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

Fraude relacionado con el empleo

El fraude relacionado con el empleo consiste en el anuncio masivo al público de ofertas de empleo u oportunidades de negocio falsas o engañosas en sitios web de ofertas de empleo[116]. Este tipo de fraude consiste en anunciar una oportunidad que es totalmente ficticia o mucho menos rentable de lo anunciado, y las víctimas pierden dinero sin recibir el empleo o la remuneración prometidos. Los autores del fraude suelen solicitar a las víctimas que realicen pagos por adelantado, antes de ocupar un puesto o crear su empresa; este pago se explica de distintas maneras, por ejemplo, por la compra o el arrendamiento de productos o equipos necesarios para establecer la empresa, la organización de viajes, la impartición de formación o la realización de comprobaciones de calificaciones crediticias[117]. En otras estafas, los autores envían anticipos mediante cheques fraudulentos para cubrir los gastos iniciales de la víctima, antes de afirmar que han pagado de más y pedir a las víctimas que les transfieran el dinero de regreso[118]. Las personas necesitadas de oportunidades económicas pueden ser especialmente vulnerables a este tipo de fraude.

El aumento sustancial de la contratación en línea aporta muchas ventajas a las empresas legítimas, entre ellas la posibilidad de dirigir las comunicaciones a un gran volumen de solicitantes de empleo y evaluar a gran número de candidatos. Sin embargo, estas mismas ventajas pueden ser aprovechadas por personas que utilizan sitios de empleo legítimos, foros en línea y redes sociales para difundir anuncios de trabajo fraudulentos entre un gran número de personas que buscan empleo. Para los portales de empleo es muy difícil detectar los anuncios fraudulentos que se publican en sus plataformas[119].

Quienes cometen fraudes se aprovechan de la demanda de puestos deseables, sobre todo entre los solicitantes de empleo que poseen menos cualificaciones o competencias, y ofrecen condiciones de trabajo (p. ej., trabajo desde casa o en condiciones flexibles) o niveles de remuneración que normalmente están

[116] Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud".

[117] Alexandrea J. Ravenelle, Erica Janko y Ken Cai Kowalski, "Good jobs, scam jobs: detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic", *New Media and Society*, vol. 24, núm. 7 (julio de 2022); y Cassandra Cross y Deanna Grant-Smith, "Recruitment fraud: increased opportunities for exploitation in times of uncertainty?", *Social Alternatives*, vol. 40, núm. 4 (2021).

[118] Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud".

[119] Mohammed A. Sofy, Mohammed H. Khafagy y Rasha M. Badry, "An intelligent Arabic model for recruitment fraud detection using machine learning", *Journal of Advances in Information Technology*, vol. 14, núm. 1 (febrero de 2023); y Syed Mahbub y Eric Pardede, "Using contextual features for online recruitment fraud detection", 27ª Conferencia Internacional sobre Desarrollo de Sistemas de Información (ISD2018), celebrada en Lund (Suecia) en 2018.

fuera de su alcance. Un estudio realizado en los Estados Unidos de América reveló que para muchos trabajadores que realizaban trabajos temporales o precarios (como en la economía del empleo ocasional) era habitual encontrarse con anuncios de empleo fraudulentos en línea[120]. La incertidumbre económica y los índices elevados de desempleo son un caldo de cultivo para el fraude relacionado con el empleo, ya que la ausencia de oportunidades en la economía legal lleva a quienes buscan empleo a tomar decisiones más desesperadas y arriesgadas[121].

Las víctimas también corren el riesgo de convertirse en objetivo repetidamente porque a muchas se les pide que faciliten información personal o documentos de identidad durante el proceso fraudulento de solicitud de empleo[122]. La principal motivación de algunos fraudes relacionados con el empleo es robar los datos personales de las víctimas. En otros casos, las propias víctimas se ven arrastradas a facilitar la delincuencia. Por ejemplo, las oportunidades de negocio fraudulentas pueden funcionar como esquemas piramidales ilegales en los que los beneficios para la víctima proceden de reclutar a otras personas para que participen[123]. Las víctimas que aceptan trabajos como mensajeros pueden verse implicadas en la entrega de mercancías de contrabando o robadas, y otras pueden verse envueltas como mulas de dinero para facilitar el blanqueo de dinero[124].

Fraude en inversiones de consumidores

El fraude en inversiones de consumidores suele implicar la comercialización y venta de títulos, incluidas acciones y bienes inmuebles, bonos estatales o empresariales, materias primas como metales preciosos y divisas[125]. Los autores engañan a sabiendas a los inversores facilitándoles información que o bien tergiversa manifiestamente los beneficios que pueden obtenerse de una inversión[126] o bien se refiere a una inversión que no existe[127].

La comisión de estos tipos de fraude puede requerir un profundo conocimiento de la normativa y los controles conexos que rigen los mercados. La línea que separa la práctica legítima de la ilegítima puede ser permeable y difícil de percibir. En algunos casos, los delincuentes explotan los mecanismos de confianza registrándose como una entidad regulada o explotando a otros agentes legítimos con estatus regulado. Al ocupar esta zona gris entre la práctica legítima y la ilegítima, crean obstáculos para los organismos encargados de hacer cumplir la ley y las entidades reguladoras, que deben sortearlos y presentar pruebas suficientes y sólidas del engaño y demostrar que se ha producido un delito[128]. De

[120] Ravenelle, Janko y Cai Kowalski, "Good jobs, scam jobs".

[121] Cross y Grant-Smith, "Recruitment fraud"; y Delali Kwasi Dake, "Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites", *International Journal of Computer Applications*, vol. 184, núm. 51 (marzo de 2023).

[122] Sofy, Khafagy y Badry, "An intelligent Arabic model".

[123] Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud".

[124] Ravenelle, Janko y Cai Kowalski, "Good jobs, scam jobs"; y Mohanamerry Vedamanikam, Saralah Devi Mariamdaran Chethiyar y Norruzeyati bt Che Mohd Nasir, "Model for money mule recruitment in Malaysia: awareness perspective", *PEOPLE: International Journal of Social Sciences*, vol. 6, núm. 2 (2020).

[125] Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud".

[126] Por ejemplo, la venta de acciones especulativas de muy bajo precio que consisten en inversiones en pequeñas empresas que ofrecen rendimientos anormales a los posibles inversionistas. Un método habitual es la estafa consistente en promocionar activamente un producto para inflar artificialmente la demanda de una acción desconocida o poco conocida, antes de que el estafador venda sus acciones para obtener grandes beneficios y otros inversionistas sufran pérdidas (Bill Hu, Thomas McInish y Li Zeng, "Gambling in penny stocks: the case of stock spam e-mails", *International Journal of Cyber Criminology*, vol. 4, núms. 1 y 2 (julio/diciembre de 2010); y Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud").

[127] Las estafas Ponzi y piramidales funcionan con principios similares, utilizando el dinero captado de nuevos inversionistas para pagar a los anteriores, pero las estafas piramidales se distinguen porque las inversiones se venden como una oportunidad de negocio y los propios inversionistas son recompensados por captar nuevos inversionistas (véase, por ejemplo, Claire Nolasco, Michael Vaughn y Rolando V. del Carmen, "Revisiting the choice model of Ponzi and Pyramid schemes: analysis of case law", *Crime, Law and Social Change*, vol. 60, núm. 4 (noviembre de 2013)).

[128] Branislav Hock y Mark Button, "Why do people join pyramid schemes?", *Journal of Financial Crime*, vol. 30, núm. 5 (2023); y Skidmore, *Protecting People's Pensions*.

hecho, aunque resulta poco ético, algunos pueden emplear métodos que causan un perjuicio a los inversionistas pero que resultan no ser delictivos. Las estafas piramidales y Ponzi[129] son modelos operativos habituales de los delincuentes, según los cuales el esquema de inversión se sostiene manteniendo un flujo continuo de inversiones de nuevos inversionistas en lugar de un rendimiento de un producto o inversión real que puede no haber existido nunca[130]. Las investigaciones han revelado que el sexo y la edad pueden afectar a la vulnerabilidad ante estos programas, muchos de los cuales se aprovechan de la brecha salarial de género y afirman que ayudan a las mujeres ofreciéndoles oportunidades económicas y un sentimiento de comunidad[131].

Quienes cometen fraudes relacionados con las inversiones hacen mucho por cultivar una apariencia de legitimidad y suelen adoptar las estructuras, los procesos y el lenguaje de una organización oficial legítima, incluida una clara división del trabajo, con una jerarquía y funciones asignadas al personal[132]. La complejidad de la operación es variable y puede depender de su duración prevista. Las denominadas operaciones "*rip and tear*" pueden funcionar durante un tiempo breve antes de desaparecer con el dinero de los inversores, mientras que otras estafas pueden operar sin ser detectadas durante muchos años[133].

Las víctimas de casos de fraude en las inversiones sufren las pérdidas más elevadas en comparación con las de otros tipos de fraudes dirigidos contra particulares. Son engañadas y se les inculcan expectativas de rentabilidad económica totalmente falsas o sumamente exageradas. Muchos inversionistas pierden todo su dinero o gran parte de él. Independientemente del método concreto que se emplee, a las víctimas se les suele vender una expectativa del valor que obtendrán de su inversión en el futuro, lo que significa que pueden pasar años desde la inversión inicial antes de que se den cuenta de que han sido defraudadas. Las particularidades de las distintas tramas y el engaño subyacente son muy diversas, pero pueden incluir lo siguiente:

- Un engaño completo, en el que el servicio o producto de inversión nunca existió
- La venta a sabiendas de acciones sin valor o sobrevaloradas para inversiones de alto riesgo que probablemente no producirán el rendimiento prometido
- Técnicas de manipulación del mercado que inflan artificialmente el valor de las inversiones ante inversores desprevenidos (véase la descripción de una estafa de salida que figura más adelante)

Las pérdidas y el impacto en las víctimas pueden depender de las metodologías empleadas por los delincuentes. Si, por ejemplo, el objetivo son los ahorros de pensiones de las personas, el impacto del fraude puede cambiar la vida de la víctima individual, mientras que algunas inversiones en criptomonedas pueden centrarse en recibir cantidades más pequeñas, pero de un mayor número de víctimas (véase el estudio de caso que se presenta más adelante). Una vez robado el dinero, la víctima puede volver a ser blanco de los mismos delincuentes u otros, que en algunos casos afirman estar afiliados a un organismo

[129] Las estafas Ponzi y piramidales funcionan con principios similares, utilizando el dinero captado de nuevos inversionistas para pagar a los anteriores, pero las estafas piramidales se distinguen porque las inversiones se venden como una oportunidad de negocio y los propios inversionistas son recompensados por captar nuevos inversionistas (véase, por ejemplo, Claire Nolasco, Michael Vaughn y Rolando V. del Carmen, "Revisiting the choice model of Ponzi and Pyramid schemes: analysis of case law", *Crime, Law and Social Change*, vol. 60, núm. 4 (noviembre de 2013)).

[130] Hock y Button, "Why do people join pyramid schemes?"; y Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[131] Li Huang *et al.*, "Gender and age-based investor affinities in a Ponzi scheme", *Humanities and Social Sciences Communications*, vol. 8, art. núm. 60 (2021); Delano Law Offices, "Pyramid schemes target females", 1 de febrero de 2022; y Taylor Walsh, "Multilevel marketing, an unwinnable lottery: how MLMs illegally target women and minorities using deceptive and predatory recruitment practices and the need for specific and expanded legal protections", *Georgetown Journal of Gender and the Law*, núm. XXIV-1 (2002).

[132] Shover, Coffey y Sanders, "Dialing for dollars".

[133] Levi, "Organized fraud and organizing frauds"; y Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

legítimo capaz de rastrear y recuperar el dinero perdido, pero se pide a la víctima que haga un pago por adelantado (el llamado fraude de recuperación)[134].

Fraude en inversiones en criptomonedas

Las modalidades del fraude en las inversiones han experimentado cambios en respuesta a las nuevas tecnologías digitales y las novedades del ámbito financiero, especialmente en los sectores financieros descentralizados que utilizan criptomonedas y la tecnología de cadenas de bloques para realizar transacciones financieras sin necesidad de la intermediación de una institución financiera (p. ej., un banco).

Así, el fraude en las inversiones de consumidores parece ir en aumento, en parte debido al incremento de los fraudes relacionados con inversiones en criptomonedas. Este nuevo medio para el fraude en las inversiones saca partido de la rapidez y agilidad que ofrecen los espacios digitales y permite a los delincuentes realizar una comercialización masiva con rapidez y a un costo relativamente bajo y, en algunos casos, aprovechar tecnologías automatizadas (o bots) para delinquir reiteradas veces[135]. En los mercados financieros nuevos, como el de las criptomonedas, las dificultades en materia de regulación crean mayores lagunas que pueden ser explotadas. Los autores suelen aprovechar los medios sociales y las aplicaciones de comunicación digital para comercializar sus productos, y en algunos casos utilizan imágenes de personas famosas o de la cultura popular para persuadir a las víctimas de que inviertan su dinero. Estos nuevos métodos de comercialización han ampliado el alcance que puede tener el fraude en las inversiones para atrapar a un mayor volumen y diversidad de inversionistas, muchos de ellos de entre 30 y 40 años de edad[136].

Los métodos que se emplean en el fraude en inversiones en criptomonedas son diversos tanto en cuanto a su complejidad técnica como en cuanto a la innovación que representan, y algunas técnicas, como las siguientes, se transponen de otros métodos como la manipulación del mercado y la seducción financiera:

- Se desarrollan y publicitan plataformas fraudulentas de inversión en criptomonedas para convencer a las víctimas de que inviertan en una criptomoneda. Al igual que ocurre con las formas tradicionales de fraude en las inversiones, la confianza de la víctima puede cultivarse a lo largo del tiempo, a veces mediante técnicas de seducción financiera (véase más adelante la sección relativa al fraude de relaciones y confianza). En algunos casos, se desarrolla un sitio web o una aplicación fraudulentos para mostrar que la inversión de las víctimas está dando buenos resultados, lo que sirve para fomentar nuevas inversiones y la captación de otros inversionistas dentro de la red social de las víctimas[137].
- Las estafas de salida implican la creación de una criptoficha falsa que puede negociarse con otras criptomonedas en un intercambio descentralizado. Una vez que un número suficiente de víctimas ha canjeado sus monedas por la criptoficha, el delincuente puede retirar todo el dinero invertido, dejando a las víctimas con una criptoficha sin valor. Una técnica concreta de "inflación y venta" sigue una lógica similar a la de una estafa piramidal o Ponzi tradicional, según la cual los estafadores inflan artificialmente el valor de la criptoficha mediante el uso de sus propios fondos y atraen a inversionistas que, a su vez, animan a otros. Este proceso puede completarse en

[134] Por ejemplo, véase Estados Unidos, Buró Federal de Investigaciones, "Increase in companies falsely claiming an ability to recover funds lost in cryptocurrency investment scams", 11 de agosto de 2023.

[135] Arianna Trozze, Toby Davies y Bennett Kleinberg, "Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering", *Journal of Forensic Science International: Digital Investigation*, vol. 46 (septiembre de 2023).

[136] Estados Unidos, Departamento de Justicia, Oficina de Asuntos Públicos, "Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes", comunicado de prensa, 3 de abril de 2023.

[137] Por ejemplo, véase Estados Unidos, Buró Federal de Investigaciones, "Scammers target and exploit owners of cryptocurrencies in liquidity mining scam", 21 de julio de 2022.

cuestión de minutos u horas y, una vez retirado el dinero, el mismo delincuente puede establecer otra criptoficha para captar a otros inversionistas incautos[138].

ESTUDIO DE CASO: INVERSIÓN FRAUDULENTA EN CRIPTOMONEDAS

Se descubrió que miembros de un grupo delictivo organizado, la mayoría de ellos ubicados en Bélgica, estaban implicados en una estafa de salida que, según la policía, había defraudado a 223.000 personas de 177 países. Los autores operaban desde un sitio web de recompensas sociales, por lo demás legítimo, y animaban a invertir en una criptomoneda específica. Empleaban una técnica de venta piramidal que recompensaba a los miembros por reclutar a otros nuevos para que se inscribieran. De este modo, los autores del fraude inflaban artificialmente el valor de la inversión. El grupo delictivo organizado o bien se retiraba con una gran cantidad de los fondos antes de que estallara la burbuja o utilizaba desinformación para inflar el valor de la criptomoneda antes de venderla para obtener una importante plusvalía. Los miembros del grupo delictivo organizado fueron hallados en posesión de 1,1 millones de euros en efectivo y 1,5 millones de euros en criptomonedas.

Fuente: Agencia de la Unión Europea para la Cooperación Policial (Europol), *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, Europol Spotlight Report Series (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2021).

Fraude mediante la suplantación de una persona u organización fiable

El fraude mediante la suplantación de la identidad de una persona u organización fiable suele consistir en la manipulación de las comunicaciones para que parezcan proceder de una persona u organización con la que las víctimas tienen, o creen tener, una relación legítima. Esto incluye organismos públicos como la policía o la autoridad fiscal, proveedores de servicios del sector privado e incluso amigos o familiares[139]. Un rasgo distintivo esencial de muchos tipos de fraude de esta categoría (aunque no todos) es el uso de técnicas de persuasión que apelan menos a los deseos y necesidades de las víctimas (como en los fraudes a los consumidores) y, en su lugar, evocan miedo, temor, ansiedad o preocupación[140]. Inducir un estado emocional exacerbado sirve para obstaculizar la toma de decisiones y hace que las víctimas sean más susceptibles a la manipulación.

El fraude por suplantación de identidad implica una serie de pretextos e hipótesis, entre los que se cuentan los siguientes:

- Suplantación de la identidad de funcionarios públicos. Los autores emplean diversas técnicas para hacerse pasar por funcionarios públicos que representan a organismos como las entidades encargadas de hacer cumplir la ley, las autoridades fiscales o los departamentos de inmigración, seguridad social o sanidad. Este fraude suele implicar amenazas de repercusiones legales u otras formas de perjuicio en caso de que la víctima no envíe un pago[141].

[138] Pengcheng Xia *et al.*, "Demystifying scam tokens on Uniswap decentralized exchange" (2021).

[139] Estados Unidos, Comisión Federal de Comercio, Data and visualizations, Data spotlight, "Impersonation scams: not what they used to be", 1 de abril de 2024.

[140] DeLiema y Witt, *Mixed Methods Analysis of Consumer Fraud Reports*.

[141] Un ejemplo consistía en un mensaje enviado por correo electrónico y a través de medios sociales que aparentaba proceder de Europol y en el que se decía a las víctimas que habían sido vistas accediendo a material de abusos sexuales a menores y que debían efectuar un pago de entre 3.000 y 7.000 euros para evitar ser procesadas (Europol, "Online fraud schemes: a web of deceit", Europol Spotlight Report Series (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2023), pág. 11).

- Suplantación de la identidad de servicios legítimos. Los autores emplean diversos pretextos, que van desde el cobro de deudas y la entrega de paquetes hasta la prestación de apoyo informático. Incluso pueden hacerse pasar por funcionarios bancarios que desean evitar la pérdida de dinero a manos de estafadores. Los autores del fraude pueden fingir representar a un proveedor de servicios con el que la víctima tiene una relación establecida (p. ej., un banco o un servicio de mensajería), o pueden adoptar una apariencia oficial para convencer a la víctima de que son legítimos; por ejemplo, pueden hacerse pasar por representantes de un bufete de abogados encargado de cobrar una deuda inexistente de la víctima[142]. Otros ejemplos importantes son los fraudes relacionados con loterías y premios, en los que se dice a las víctimas que han ganado una lotería u otro juego y se las convence de que deben realizar un pago para acceder a los fondos[143]. Se aducen diversas razones, entre ellas una supuesta comisión de tramitación, transferencia o gestión o cargas fiscales. Sin embargo, una vez efectuado el pago, las víctimas no reciben el premio prometido. Las técnicas más comunes incluyen la suplantación de una autoridad pública, una organización de loterías o premios conocida o una lotería en el extranjero[144]. En otros ejemplos, los autores del fraude dicen representar a organizaciones benéficas en campañas de publicidad masiva para obtener donaciones de las víctimas[145]. Las personas que se encuentran en situación vulnerable, incluidas las personas de edad y las personas con discapacidad, pueden estar especialmente expuestas a este tipo de fraude debido a su dependencia de los servicios sociales y a sus mayores niveles de aislamiento social, como se ha visto en el estudio de caso sobre productos y servicios de consumo y fraude en las inversiones del capítulo anterior.
- Fraude del apoyo técnico. Es muy frecuente en algunas regiones, como América del Norte y Europa, y gran parte de los casos tienen su origen en la India[146]. Suelen consistir en que el estafador se hace pasar por una empresa de *software* legítima para convencer a las víctimas de que sus dispositivos están en peligro y necesitan asistencia técnica (p. ej., por una infección con un programa malicioso). A continuación, se persuade a las víctimas para que proporcionen acceso remoto a su dispositivo, antes de pedirles una tarifa por la prestación de un servicio ficticio[147]. En algunos casos, se realizan cargos adicionales en las cuentas de las víctimas, se instalan programas maliciosos en sus dispositivos o se pueden robar sus datos personales. Algunas empresas fraudulentas adoptan métodos similares al fraude al consumidor mediante la publicidad masiva de servicios de asistencia técnica a través de sitios web que imitan a proveedores de servicios legítimos.
- Suplantación de la identidad de un amigo o familiar. Normalmente se trata de mensajes en los que se inventa una situación en la que la persona se encuentra en alguna dificultad de carácter urgente, como estar en el hospital, haber sufrido un accidente o haber sido detenida, y se afirma que puede resolverse si la víctima envía una cantidad concreta de dinero. A menudo,

[142] Véase, por ejemplo, Estados Unidos, Comisión Federal de Comercio, "Phantom debt collectors permanently banned from industry in FTC settlement", comunicado de prensa, 13 de diciembre de 2021.

[143] Mortley, "A crime of opportunity".

[144] En un caso, se enviaron comunicaciones fraudulentas en las que se afirmaba proceder de una empresa que había sido designada por la Organización Mundial de la Salud (OMS) para administrar un plan de compensación mediante una lotería. Se informó a los destinatarios de que habían sido seleccionados como beneficiarios o ganadores de un pago de un premio de lotería de compensación por las pérdidas y daños sufridos durante la pandemia de COVID-19 (OMS, "Fraudulent 'COVID-19 Compensation Lottery Prize' scam, falsely allegates association with WHO and others", comunicado de prensa, 6 de agosto de 2021). Véase también Estados Unidos, Comisión Federal de Comercio, "Fake prize, sweepstakes, and lottery scams", mayo de 2021.

[145] Por ejemplo, estafas comercializadas mediante páginas web y correos electrónicos fraudulentos, que pretenden apoyar a Ucrania o a los ucranianos afectados por el conflicto armado, en algunos casos suplantando los dominios de organizaciones humanitarias (véase Europol, "Online fraud schemes").

[146] Liu *et al.*, "Understanding, measuring, and detecting"; véase también Estados Unidos, Oficina de Asuntos Públicos, "Dozens of individuals indicted in multimillion-dollar Indian call center scam targeting U.S. victims", comunicado de prensa, 27 de octubre de 2016.

[147] Najmeh Miramirkhani, Oleksii Starov y Nick Nikiforakis, "Dial one for scam: a large-scale analysis of technical support scams", ponencia de conferencia, Network and Distributed System Security Symposium, celebrado en San Diego (California, Estados Unidos), del 26 de febrero al 1 de marzo de 2017.

el delincuente se hace pasar por hijo o nieto de la víctima[148]. Algunas estafas consisten en utilizar datos personales de las publicaciones en las redes sociales del amigo o pariente para que la comunicación resulte más convincente, por ejemplo, sabiendo que está de vacaciones en un lugar determinado. Entre los ejemplos emergentes se incluyen los delincuentes que utilizan inteligencia artificial generativa para clonar la voz de un amigo o familiar en una llamada telefónica a la víctima, lo que despierta una respuesta aún más fuerte o visceral en la víctima[149].

Los tipos de fraude antes mencionados suelen implicar la comunicación masiva mediante correo electrónico basura, redes sociales, mensajes de texto o llamadas telefónicas automatizadas que utilizan un mensaje grabado. Estas tecnologías facilitan el contacto casi simultáneo con miles de víctimas a la vez, lo que les da un alcance inmenso[150]. Algunos grupos delictivos organizados operan desde centros de llamadas, en los que los operadores de llamadas se hacen pasar por representantes de organismos gubernamentales o marcas de empresas conocidas. Hay indicios que sugieren que los adultos mayores son objetivos de fraudes como la suplantación de la identidad de una entidad gubernamental o el fraude de apoyo técnico y resultan especialmente vulnerables a ellos[151].

Falsificación de identidad

La falsificación de identidad implica el uso de información de identidad robada o falsa para acceder directamente a bienes, servicios o dinero de las víctimas. La información robada puede utilizarse para realizar compras o acceder a cuentas financieras. Este fraude puede perpetrarse sin que medie comunicación directa con la persona cuya identidad está siendo usurpada ni una acción directa alguna por parte de ella, ya que el objetivo del engaño suele ser el proveedor de los bienes, servicios o dinero (p. ej., un banco o vendedor). De este modo, el daño se reparte entre diferentes actores, a saber, la víctima cuya identidad es objeto de abuso, el proveedor de servicios financieros u otra empresa de la que se sustrae el dinero y, en algunos casos, el proveedor de los bienes o servicios adquiridos con los fondos robados.

La manipulación y el abuso de la identidad pueden cumplir diversas funciones en la comisión de delitos organizados, además de perpetrar fraude, incluida la obstrucción de intentos por rastrear la actividad delictiva hasta los autores[152]. Del mismo modo, desempeñan un papel clave a la hora de facilitar los engaños empleados en tipos de fraude como el romántico y el fraude al consumidor[153]. La presente sección se centra en las metodologías específicas en cuyo marco se utiliza información de identidad robada o falsa para obtener acceso directo a bienes, servicios o dinero de las víctimas; por ejemplo, el uso de información robada para hacer compras o acceder a cuentas financieras. La víctima en muchos de estos casos es la empresa engañada para que suministre financiación, bienes o servicios a la persona que comete el fraude.

Es importante señalar que la falsificación de identidad no está supeditada a la implicación de grupos delictivos organizados. Por ejemplo, la suplantación del titular de una tarjeta requiere poco más que un bolso robado y una tienda local para hacer una compra rápida. No obstante, las habilidades y los

[148] Estados Unidos, Buró Federal de Investigaciones, "The grandparent scam: don't let it happen to you", 2 de abril de 2012.

[149] Alvaro Puig, "Scammers use AI to enhance their family emergency schemes", Comisión Federal de Comercio, 20 de marzo de 2023.

[150] Un ejemplo común consiste en el uso de mensajes fraudulentos que dicen proceder de la administración de la seguridad social. En 2020, una estafa de este tipo se dirigió a casi la mitad de todos los adultos de Estados Unidos durante un período de tres meses (DeLiema y Witt, *Mixed Methods Analysis of Consumer Fraud Reports*, pág. 2).

[151] Liu *et al.*, "Understanding, measuring, and detecting"; Lei Yu *et al.*, "Vulnerability of older adults to government impersonation scams", *JAMA Network Open*, vol. 6, núm. 9 (septiembre de 2023); y DeLiema y Langton, "Older victims of mass marketing scams".

[152] Baechler, "Document fraud".

[153] Véase, por ejemplo, Cassandra Cross y Rebecca Layt, "'I suspect that the pictures are stolen': romance fraud, identity crime, and responding to suspicions of inauthentic identities", *Social Science Computer Review*, vol. 40, núm. 4 (agosto de 2022).

recursos de que disponen los grupos delictivos organizados aumentan enormemente la capacidad para perpetrar fraudes mediante la falsificación de identidad a gran escala y lograr elevados beneficios. Lo que vuelve especialmente grave esta amenaza es la proliferación de posibles víctimas disponibles en las economías digitales en expansión.

Hay diferentes tipos de información sobre la identidad que pueden adquirirse y cada una de ellas puede explotarse de maneras distintas: la información personal que conforma las identidades digitales en diferentes entornos en línea, como los nombres o las fechas de nacimiento; datos de cuentas financieras, como números de tarjetas de crédito; información sobre cuentas en línea, como nombres de usuario y contraseñas; y datos biométricos, como una huella digital robada de un dispositivo electrónico[154].

Los datos robados pueden utilizarse para adquirir bienes y servicios, presentar solicitudes de préstamos y otro tipo de financiación o acceder a las cuentas de las víctimas y transferir dinero desde ellas. Entre los recursos y técnicas que pueden emplear los delincuentes para acceder a la información personal con miras a cometer fraude figuran los siguientes:

- Intrusión en un sistema. Algunos delincuentes se dedican a la adquisición de información personal mediante técnicas ilícitas de piratería informática, el despliegue de programas maliciosos o la suplantación de identidad o *phishing* (para más detalles, véase la sección relativa a la usurpación de identidad).
- Mercados delictivos en línea. Existe una dinámica economía informal implicada en la compraventa de datos personales, que puede ser explotada por quienes cometen fraude mediante la falsificación de identidad[155]. La oportunidad de adquirir información de esta manera elimina algunos de los obstáculos técnicos para quienes cometen el fraude, que de otro modo no dispondrían de estas capacidades para robar información personal.
- Ingeniería social. A menudo se consigue mediante un anuncio u otra comunicación no solicitada enviados por correo electrónico u otros medios en línea, mensaje de texto o llamada telefónica no solicitada, a través de los cuales se engaña a las víctimas para que faciliten información personal. El grado de sofisticación es variable, pero los métodos más complejos, como la suplantación de sitios web legítimos, pueden proporcionar a los delincuentes acceso directo a cuentas en línea (véase el estudio de caso que se presenta más adelante).

Se emplean diversas técnicas para cometer falsificaciones de identidad. Los principales métodos son la apropiación de cuentas, el fraude sin presencia de tarjeta y el fraude en la presentación de solicitudes.

Fraude por apropiación de cuentas

En el fraude por apropiación de cuentas, los delincuentes obtienen credenciales legítimas para acceder a cuentas de usuarios. Puede tratarse de cuentas bancarias, pero también de otros tipos de cuentas financieras (p. ej., proveedores de moneda virtual), sitios de venta al por menor o cualquier proveedor de bienes y servicios. El uso de las credenciales de las cuentas robadas de las víctimas hace que las transacciones u otras actividades del delincuente sean difíciles de distinguir de las del titular real de la cuenta. La cuenta puede aprovecharse para diversos fines, como la transferencia directa de fondos a cuentas controladas por los delincuentes o la compra fraudulenta de bienes o servicios. En algunos casos, adquirir información para acceder a la cuenta de una víctima es el primero de una serie de pasos necesarios para acceder al dinero, bienes o servicios a través de intrusiones posteriores en el sistema. Esas medidas incluyen adaptaciones para superar la autentificación de dos factores dirigida a impedir

[154] Europol, "Online fraud schemes"; y Bert-Jaap Koops, Katja de Vries y Mireille Hildebrandt, eds., *D7.14b: Idem-Identity and Ipse-Identity in Profiling Practices*, Future of Identity in the Information Society Report, núm. 507512 (2009).

[155] Yip, Shadbolt y Webber, "Why forums?".

el acceso ilegítimo a las cuentas. Esto ha llevado a los delincuentes a desplegar técnicas y tecnologías adicionales, entre ellas:

- Intercambio de SIM, que consiste en engañar a un proveedor de telecomunicaciones para que transfiera el número de teléfono de la víctima a una tarjeta SIM en poder del delincuente. Esto permite a los delincuentes eludir las protecciones de autentificación de dos factores de los proveedores de servicios financieros para acceder directamente a una cuenta. Un grupo de España logró realizar transferencias fraudulentas por valor de 3 millones de euros desplegando un troyano bancario u otro programa malicioso para acceder a las credenciales bancarias en línea de las víctimas, solicitando a los proveedores de telecomunicaciones un duplicado de las tarjetas SIM de las víctimas para interceptar los códigos de autentificación enviados por el banco y transfiriendo después los fondos a las cuentas de las mulas de dinero[156].
- Atacar métodos de pago alternativos, como las tarjetas de crédito "tokenizadas" utilizadas en los servicios de pago móvil y en las billeteras electrónicas, mediante los cuales los delincuentes pueden interceptar las contraseñas de un solo uso enviadas por las entidades bancarias para autorizar una transferencia de fondos y, de este modo, realizar compras u obtener dinero[157].

Es habitual que se sustraigan fondos de cuentas mediante transferencias digitales a cuentas controladas por los delincuentes. Sin embargo, los grupos delictivos organizados también pueden hacerse con elementos de identificación físicos como tarjetas bancarias o identificaciones falsas para acudir en persona al banco y retirar dinero[158].

ESTUDIO DE CASO: FRAUDE BANCARIO

En el Reino de los Países Bajos, un grupo atacó dos bancos para acceder a las cuentas bancarias de sus clientes. El grupo estaba formado por ocho miembros principales y otras personas periféricas que facilitaban el fraude. Se enviaba un correo electrónico de *phishing* en el que se pedía a los clientes que facilitaran información o hicieran clic en un enlace que les enviaba a un sitio web controlado por los delincuentes que simulaba ser el sitio web oficial del banco. De este modo, adquirían los datos de los clientes para acceder a sus cuentas bancarias en línea. Pocos días después, los delincuentes llamaban por teléfono a las víctimas y les decían que se había implantado una nueva medida de seguridad en el banco y les pedían que facilitaran el código de transacción única para garantizar la seguridad de su cuenta. Una vez facilitado el código, el delincuente realizaba una serie de transferencias bancarias desde las cuentas de los clientes. El dinero se transfería a las cuentas de mulas de dinero para romper el rastro financiero y luego se retiraba rápidamente.

Fuente: Eric Rutger Leukfeldt, "Cybercrime and social ties: phishing in Amsterdam", *Trends in Organized Crime*, vol. 17, núm. 4 (diciembre de 2014).

Fraude sin presencia de tarjeta

Las transacciones sin presencia física de tarjeta son compras no autorizadas realizadas a distancia a un vendedor, ya sea por Internet o por teléfono. La adquisición de las credenciales financieras de una víctima

[156] Europol, *Internet Organised Crime Threat Assessment 2020* (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2020), pág. 44.
[157] Europol, "Online fraud schemes", pág. 15.
[158] Véase, por ejemplo, UK Finance, "Organised crime group sentenced following over £1 million conspiracy to defraud", comunicado de prensa, 6 de noviembre de 2023.

es suficiente para engañar tanto al proveedor de servicios financieros como al vendedor, sin necesidad de una interacción directa con la víctima ni de acceder a la tarjeta de pago física. Existe una floreciente economía subterránea en la que ciberdelincuentes con capacidad para adquirir esta información en grandes cantidades (p. ej., mediante una violación de datos) pueden venderla a posibles estafadores para obtener una ganancia. A modo de ejemplo, se descubrió que un sitio web investigado por la policía contenía 150.000 números robados de tarjetas de crédito de 1.300 bancos, la mayoría obtenidos mediante intrusión en un sistema; la venta de estos datos a personas que cometieron fraudes había provocado la pérdida de 20 millones de dólares de cuentas abiertas en los Estados Unidos[159]. Quienes falsifican la identidad de otra persona suelen requerir una serie de pasos clave para aprovecharse de las credenciales financieras de una víctima, algunos de los cuales pueden implicar a otros coautores, que pueden estar en línea o vivir en la misma localidad. Entre las etapas clave de este fraude cabe citar las siguientes:

- Adquirir conocimientos y recursos de otros miembros de grupos en línea
- Obtener credenciales financieras de grupos en línea
- Disfrazar los pedidos para evitar que se activen los algoritmos de detección de fraude en un sitio comercial; esto puede implicar la realización de múltiples pedidos más pequeños para que se entremezclen con los pedidos legítimos
- Recibir los pedidos en una dirección que no pueda ser rastreada a los autores del fraude —puede tratarse de una propiedad desocupada o de la dirección de una "mula"—; otra posibilidad es utilizar a una persona infiltrada en la empresa de reparto para interceptar el artículo
- Revender los artículos como vendedor individual o venderlos al por mayor haciéndose pasar por un comerciante legítimo en los cibermercados convencionales[160]

ESTUDIO DE CASO: FRAUDE SIN PRESENCIA DE TARJETA

Una red de delincuentes utilizaba datos de tarjetas de crédito robadas para realizar compras fraudulentas en sitios web comerciales. Adquirían estos datos de dos formas: a) obteniéndolos y comprándolos en foros en línea utilizados para este fin, y b) robando la información a un exempleador. Los delincuentes también se encontraron en posesión de clonadores[a] de cajeros automáticos que podrían utilizarse para recopilar más datos de tarjetas. Un paso preparatorio clave consistió en piratear cuentas de clientes en sitios web comerciales y modificar su información de contacto, con lo que los titulares de las tarjetas no serían notificados de las compras realizadas por los delincuentes. Los productos se compraban y entregaban en los puntos de recogida de paquetes y se recogían utilizando documentos de identidad falsos o "mulas" alistadas para ese fin. La policía identificó unos 2.000 pedidos realizados en sitios web de compras, por un valor estimado de hasta 60.000 euros. A continuación, los productos se revendían en sitios web comerciales.

[a] Un dispositivo que se acopla a un cajero automático para robar la información de las tarjetas.

Fuente: Tribunal de grande instance de París, sentencia, 20 de noviembre de 2018 (TGI Paris, 13e ch. corr., jugement du 20 novembre 2018), disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

[159] *United States of America v. Burkov*, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

[160] Bodker *et al.*, "Card-not-present fraud".

Fraude en la presentación de solicitudes

Al igual que en el fraude sin presencia de tarjeta, el fraude en la presentación de solicitudes se aprovecha de la amplia disponibilidad de información personal, que en este caso se utiliza para solicitar créditos en nombre de la víctima. Suele hacerse con el objetivo de obtener un préstamo de un proveedor de servicios financieros. Los delincuentes deben acceder a un conjunto de datos personales (p. ej., nombre, dirección y fecha de nacimiento) para poder suplantar de forma creíble a otra persona. Una tendencia emergente es el uso de la tecnología para crear identidades artificiales combinando elementos de identificación reales y falsos; una vez establecidas, estas identidades pueden cultivarse para que sean más solventes antes de utilizarse para presentar solicitudes de productos financieros de alto valor. La asociación entre la delincuencia organizada y el fraude hipotecario está reconocida desde hace tiempo y suele ser facilitada por profesionales como corredores de préstamos hipotecarios, tasadores de bienes inmuebles, contables, abogados y agentes de garantía[161]. El fraude hipotecario constituye un medio de blanquear el producto de otro delito (p. ej., el suministro de drogas), pero también puede utilizarse para generar beneficios ilícitos. Entre los métodos más comunes figuran la contratación de hipotecas utilizando los datos de otra persona o los de una persona fallecida, o la contratación de varias hipotecas para una misma dirección[162].

Fraude basado en las relaciones y la confianza

Los procesos para establecer la confianza desempeñan una función decisiva en cualquier tipo de fraude. Sin embargo, en el caso del fraude basado en las relaciones y la confianza, los delincuentes utilizan técnicas específicas para fomentar y aprovechar el poder de una relación personal con objeto de desarrollar la confianza necesaria para manipular y engañar a las víctimas[163]. En este tipo de fraude, la víctima no espera recibir un producto o servicio, sino entablar una relación genuina con el delincuente[164]. La complejidad del fraude reside menos en la explotación de sistemas técnicos o tecnológicos que en la dinámica de la relación entre la víctima y el autor.

Muchos autores de fraudes establecen relaciones en línea y utilizan diversas técnicas de ingeniería social durante meses o incluso años para ganarse la confianza de la víctima. Las víctimas habitualmente esperan entablar una relación romántica, pero la relación también puede adoptar otras formas, como una amistad de confianza, o incluso el deseo de una relación con un familiar de la víctima. Varios estudios han detectado vulnerabilidades en la población de edad avanzada relacionadas con factores como la soledad, el aislamiento social y el deseo de entablar nuevas relaciones. Otras características interseccionales, como la condición de ciudadano de un país o la discapacidad, pueden aumentar la vulnerabilidad ante estos delitos. Los delincuentes buscan y explotan esta vulnerabilidad mediante un proceso de amistad o compromiso romántico visitando a la víctima en persona (p. ej., haciéndose pasar por trabajadores), hablando por teléfono o comunicándose en línea[165].

Independientemente de las características de las víctimas, el impacto de un fraude basado en las relaciones y la confianza puede ser considerable. Si bien las víctimas experimentan pérdidas económicas, también sufren como resultado de la ruptura de la confianza y la pérdida de una relación personal

[161] May y Bhardwa, *Organised Crime Groups Involved in Fraud*; y Reurink, *Financial Fraud*.

[162] May y Bhardwa, *Organised Crime Groups Involved in Fraud*.

[163] Cassandra Cross, "Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud", *Current Issues in Criminal Justice*, vol. 36, núm. 3 (2024).

[164] Beals, DeLiema y Deevy, "Framework for a taxonomy of fraud".

[165] Cassandra Cross, " 'They're very lonely': understanding the fraud victimisation of seniors", *International Journal for Crime, Justice and Social Democracy*, vol. 5, núm. 4 (2016); y Phillips, "From 'rogue traders' to organized crime groups".

importante[166]. Además, pueden padecer importantes daños psicológicos y emocionales. Algunas pueden incluso negarse a aceptar que son o han sido víctimas de un fraude.

Fraude romántico

Una forma común de fraude basado en las relaciones y la confianza es el fraude romántico, en el cual los delincuentes construyen relaciones en línea para facilitar el engaño con la intención de embaucar a las víctimas para que les envíen dinero[167]. Las pérdidas económicas que sufren las personas en cuestión pueden ser importantes (véase el estudio de caso que se presenta más adelante). Este tipo de fraude afecta a víctimas de muchas regiones diferentes del mundo y se aprovecha del crecimiento de las redes sociales en línea y, más concretamente, de una tendencia social más amplia a encontrar relaciones románticas en línea. La aproximación inicial suele producirse a través de medios sociales o sitios web o aplicaciones de citas por parte de un delincuente que utiliza una identidad falsa junto con el historial correspondiente en su perfil[168]. Un único delincuente puede ir adoptando diversas identidades para captar y atraer a posibles víctimas; por ejemplo, una imagen de perfil femenino seductora para atraer a hombres heterosexuales o un perfil masculino que lo presente como un hombre perteneciente a una élite, glamuroso y digno de confianza (p. ej., un integrante de las fuerzas armadas)[169]. Las siguientes siete etapas clave se observan con frecuencia en los fraudes románticos:

- El deseo de la víctima de encontrar pareja
- La presentación de un perfil ideal a la víctima
- El proceso de captación
- El golpe
- La continuación del fraude
- Abuso sexual
- Nueva victimización[170]

Una vez establecida la relación, el delincuente puede solicitar inicialmente una pequeña suma de dinero antes de pedir cantidades mayores, a menudo haciendo referencia a una situación de crisis que sirve para aplicar presión a la víctima y generar en ella un sentimiento de urgencia (p. ej., una emergencia de salud o la necesidad urgente de viajar)[171]. Si se intercambiaron imágenes sexuales, también se puede extorsionar a la víctima para extraer dinero de ella. Por lo general, se pide a las víctimas que transfieran dinero a terceros países o que utilicen una tarjeta regalo o de prepago, y posteriormente pueden ser objeto de otros tipos de fraude o incluso ser reclutadas para ayudar a estafar a otras víctimas (p. ej., utilizándolas como mulas de dinero)[172].

Fraude de inversión en criptoconfianza

Una encarnación más reciente de este método ha consistido en mezclar el fraude romántico con el fraude relacionado con inversiones en criptomonedas. El fraude de inversión en criptoconfianza (bautizado en

[166] Monica T. Whitty y Tom Buchanan, "The online romance scam: a serious cybercrime", *Cyberpsychology, Behavior and Social Networking*, vol. 15, núm. 3 (marzo de 2012).

[167] Coluccia *et al.*, "Online romance scams".

[168] Cross y Layt, "'I suspect that the pictures are stolen'".

[169] Suleman Lazarus *et al.*, "What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021)", *Journal of Economic Criminology*, vol. 2 (2023).

[170] Monica T. Whitty, "The scammer's persuasive techniques model: development of a stage model to explain the online dating romance scam", *The British Journal of Criminology*, vol. 53, núm. 4 (julio de 2013).

[171] Cassandra Cross y Thomas J. Holt, "The use of military profiles in romance fraud schemes", *Victims and Offenders*, vol. 16, núm. 3 (2021).

[172] Europol, "Online fraud schemes".

muchos medios de comunicación como fraude de "matanza de cerdos" o *pig butchering*[173]) implica que un delincuente fomente una relación personal con una víctima en línea. En lugar de inventar una situación de crisis, los delincuentes establecen una relación íntima con la víctima y a continuación se aprovechan de su confianza para atraerla a un plan de inversión fraudulento. Los delincuentes pueden desarrollar un sitio web o una aplicación fraudulentos a los que puede acceder la víctima, e incluso ofrecer un "servicio de atención al cliente" para los inversionistas[174]. La integración de las inversiones en criptomonedas en el engaño tiene una serie de consecuencias: amplía el grupo de posibles víctimas para incluir a las de grupos de edad más jóvenes, introduce a las víctimas en un mercado desconocido, inestable y de alto riesgo, lo que significa que es menos probable que reconozcan que son víctimas de fraude, e introduce más dificultades para que los investigadores de delitos rastreen los fondos hasta los delincuentes[175].

Gran parte de la investigación sobre el fraude romántico se ha centrado en las víctimas y sus experiencias, no en los delincuentes, que son menos visibles[176]. Muchos son delitos transnacionales y a menudo (aunque no siempre) son perpetrados por grupos delictivos organizados. El estudio de caso sobre fraude romántico que se presenta a continuación ofrece un ejemplo en el que un grupo delictivo organizado tuvo como objeto de fraude a una víctima situada en otro país durante un período de tiempo prolongado.

ESTUDIO DE CASO: FRAUDE ROMÁNTICO

Tres delincuentes dirigieron sus actividades contra una mujer residente en Australia a lo largo de tres años. El contacto inicial se realizó a través de un sitio web de búsqueda de pareja, tras lo cual se mantuvo la comunicación por correo electrónico y por teléfono. Los delincuentes adoptaron la identidad de un ciudadano alemán residente en Australia pero que trabajaba desde Ghana. Para obtener fondos de la víctima, le presentaron múltiples situaciones a lo largo del tiempo, desde la necesidad de ayuda para despachar mercancías importadas en un puerto hasta problemas de salud. En varios momentos, el delincuente inicial presentó a la víctima a otros delincuentes, alegando que eran socios suyos; la víctima se comunicó con cada uno de ellos y se le pidió ayuda financiera para remediar una situación urgente. La víctima estaba motivada para ayudar al agresor inicial, con el que creía que mantenía una relación romántica, a regresar a Australia. En total, la víctima perdió casi 450.000 dólares australianos en este fraude.

Fuente: *Republic v. Mohammed Libabatu, Charles Mensah and Nurudeen Alhassan*, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

Fraude contra empresas u organizaciones

El fraude contra empresas u organizaciones suele implicar el abuso de sistemas internos o de una relación comercial para defraudar a la víctima. El fraude puede ser perpetrado por alguien interno o externo a la organización, como personal, clientes o proveedores, personas pertenecientes a la organización que actúan en connivencia con autores externos, o delincuentes externos que explotan los servicios o sistemas de la empresa u organización[177]. Este tipo de fraude puede perpetrarse tanto desde el interior

[173] No se recomienda el uso de esta frase por las connotaciones negativas que tiene para las víctimas.

[174] Fangzhou Wang y Xiaoli Zhou, "Persuasive schemes for financial exploitation in online romance scam: an anatomy on sha zhu pan (杀猪盘) in China", *Victims and Offenders*, vol. 18, núm. 5 (2023).

[175] Cross, "Romance baiting, cryptorom and 'pig butchering'".

[176] Lazarus *et al.*, "What do we know about online romance fraud studies?".

[177] Duffield y Grabosky, *The Psychology of Fraud*.

de empresas legítimas, como por actores o con productos también legítimos, en lugar de tratarse de tramas diseñadas desde el principio para cometer fraude.

El fraude perpetrado por personal interno suele implicar el abuso de sistemas internos o de una relación comercial para defraudar a un empleador, socio comercial u otra parte interesada. Este tipo de fraude incluye grandes fraudes empresariales, que suelen ser perpetrados por personal en puestos directivos que engañan a los inversionistas o a otras partes interesadas clave[178]. El fraude en los estados financieros engloba diversos métodos para falsear la verdadera naturaleza o salud financiera de una empresa, fondo o producto de inversión con el fin de engañar y distorsionar las percepciones de otras personas, como inversionistas, reguladores y otros agentes del mercado, sobre su salud financiera y perspectivas futuras[179]. Tipos similares de fraude contable también pueden encubrir la apropiación indebida, la malversación o el desfalco de fondos. Este tipo de fraude puede perpetrarse en respuesta a presiones para cumplir las expectativas de rendimiento y puede ser llevado a cabo por ejecutivos de empresas, operadores financieros o administradores de fondos de inversión libre que informan sobre el rendimiento financiero.

La motivación delictiva de este tipo de fraude puede derivarse de diversas circunstancias, algunas de ellas relacionadas con las condiciones imperantes en la empresa o el sector. Algunos ejemplos son los directores de empresas que responden a dificultades financieras o una cultura del lugar de trabajo que fomenta una actitud permisiva con el fraude o que impone altas expectativas y grandes presiones para lograr resultados financieros. En muchos casos de fraude contra empresas u organizaciones puede resultar difícil distinguir las prácticas fraudulentas de las legítimas (aunque éticamente dudosas).

El fraude contra empresas u organizaciones suele tener por objeto defraudar a una empresa u organización concreta, pero en algunos casos puede tener repercusiones de mayor alcance en el sector, incluidos los consumidores del mercado. No es infrecuente que este tipo de fraude se produzca durante períodos de tiempo prolongados, y puede acarrear importantes pérdidas financieras a empresas y organizaciones. Sin embargo, las reducidas penas impuestas a quienes cometen fraude de cuello blanco y la mayor capacidad entre los autores de fraude que ocupan posiciones legítimas y de confianza para perpetrar fraudes graves sin recurrir a coautores pueden limitar el papel de los grupos delictivos organizados en determinados contextos[180].

El fraude en el que intervienen agentes externos que se aprovechan de relaciones comerciales o de otro tipo con la empresa u organización víctima incluye:

- Los fraudes con sociedades a corto o largo plazo pueden ser perpetrados por empresas de comercio existentes o por empresas adquiridas o creadas con fines fraudulentos. Las empresas establecen un historial de crédito, confianza o credibilidad, que se utiliza con objeto de engañar a un comprador, vendedor o acreedor para que suministre bienes o financiación. Esto se hace a sabiendas de que no se puede pagar o sin intención de hacerlo[181]. Algunos autores de fraude abusan de los sistemas de confianza que facilitan el comercio internacional. Se utilizan habitualmente cartas de crédito para realizar pagos en el comercio internacional, por lo que un banco actúa como fiador del comprador en una transacción. Los compradores fraudulentos crean sus propias entidades bancarias falsas para que actúen como fiadores a fin de defraudar a los vendedores[182]. Los vendedores envían la mercancía y no reciben ningún pago.

[178] Paolo Campana, "When rationality fails: making sense of the 'slippery slope' to corporate fraud", *Theoretical Criminology*, vol. 20, núm. 3 (agosto de 2016). Véase también Estados Unidos, Departamento de Justicia, División Penal, "Securities and commodities fraud", 11 de agosto de 2023.

[179] Reurink, *Financial Fraud*.

[180] Levi, "Organized fraud and organizing frauds"; y Levi, "Hitting the suite spot".

[181] Michael Levi, "The craft of the long-firm fraudster: criminal skills and commercial responses", en *Crime at Work: Increasing the Risk for Offenders*, vol. 2, Martin Gill, ed. (Londres, Palgrave Macmillan, 1998).

[182] Reurink, *Financial Fraud*.

- El fraude en las adquisiciones o a proveedores, que engloba diversos métodos para conseguir contratos comerciales o el pago de bienes y servicios. Esto puede implicar que los proveedores presenten declaraciones falsas[183] o, en algunos casos, la corrupción de empleados que esperan un pago por facilitar los contratos y los fondos, y adquieren así los bienes y servicios mediante engaño. En un ejemplo, una empresa constructora del Reino de los Países Bajos firmó un contrato inmobiliario con un fondo de pensiones pero, a lo largo de un período de 10 años, los gestores del contrato inflaron los contratos en millones de euros[184].

ESTUDIO DE CASO: FRAUDE EN LOS ESTADOS FINANCIEROS

Los autores, procedentes de múltiples bancos de Alemania, Francia y el Reino Unido de Gran Bretaña e Irlanda del Norte, habían intentado manipular el tipo europeo de oferta interbancaria (euríbor). Estos tipos publicados son las estimaciones que facilitan los bancos sobre el costo de pedir un préstamo a otros bancos en el mercado interbancario en un día concreto. Se utilizan como referencia para las operaciones de préstamo e influyen en los tipos de interés de los préstamos, hipotecas y cuentas de ahorro que los bancos ofrecen a sus clientes. Los delincuentes condenados presentaban estimaciones falsas de los tipos de interés con la intención de mover el índice de referencia en la dirección que más beneficiara a su empleador o a ellos mismos. Las ganancias producto del delito fueron considerables, y uno de los coautores obtuvo personalmente 57,8 millones de libras de la manipulación de los tipos. Además, sus acciones sirvieron para socavar la integridad del sistema financiero.

Fuentes: Reino Unido, Fiscalía de Delitos Económicos Graves, "Senior bankers sentenced to 9 years for rigging EURIBOR rate", 1 de abril de 2019; y Rubén Herrera *et al.*, "The manipulation of Euribor: an analysis with machine learning classification techniques", *Technological Forecasting and Social Change*, vol. 176, art. núm. 121466 (marzo de 2022).

ESTUDIO DE CASO: FRAUDE CON SOCIEDADES A LARGO PLAZO

El director general y dos altos ejecutivos de una empresa siderúrgica del Reino Unido de Gran Bretaña e Irlanda del Norte defraudaron por 500 millones de dólares a 20 bancos de financiación de operaciones comerciales de varios países. Durante un período de dos años, obtuvieron préstamos a corto plazo facilitando información engañosa y contratos falsos para pedidos de envíos de acero inexistentes. Utilizaron una empresa de transporte interna registrada en el extranjero para certificar los documentos de expedición falsos. Los préstamos mejoraron las finanzas de la empresa, lo que les permitía seguir operando. La empresa eludió el pago de los préstamos hasta que finalmente quebró, dejando grandes cantidades de deuda impagada con los bancos. Los coautores fueron condenados y el director general recibió una pena de seis años y medio de prisión.

Fuente: Reino Unido, Fiscalía de Delitos Económicos Graves, "Serious Fraud Office secures three convictions in $500 million trade finance fraud", 2 de febrero de 2023.

[183] Por ejemplo, un grupo de cuatro estafadores defraudó sistemáticamente a una plataforma de comercio electrónico manipulando el sistema de proveedores para inducir a la empresa a pagar por productos que no había pedido (Fiscalía de los Estados Unidos, Distrito Sur de Nueva York, "Four individuals charged with $19 million fraudulent invoicing scheme targeting Amazon's vendor system", comunicado de prensa, 19 de agosto de 2020).

[184] Philip Gounev, Tihomir Bezlov y Comisión Europea, Dirección General de Migración y Asuntos de Interior, *Examining the Links between Organized Crime and Corruption* (Bruselas, Oficina de Publicaciones, 2010), pág. 121.

Los grupos delictivos organizados también pueden defraudar a empresas sin ocupar una posición legítima o aparentemente legítima en los negocios. En cambio, estos tipos de fraude se perpetran mediante la intrusión en el sistema por parte de ciberdelincuentes o abusando de los servicios que la organización víctima presta a los clientes.

Fraude mediante la vulneración del correo electrónico empresarial

El fraude mediante la vulneración del correo electrónico empresarial se dirige a sociedades comerciales, pequeñas empresas y organizaciones de diversos sectores. Es una de las formas de fraude organizado más extendidas en todo el mundo[185]. Los autores de este tipo de fraude utilizan diversas técnicas de ingeniería social para convencer al personal de que realice transferencias no autorizadas de fondos a cuentas que controlan. El primer paso consiste en infiltrarse en los sistemas de comunicación de una organización para ayudar a convencer a los destinatarios de que los correos electrónicos enviados son legítimos: los métodos clave incluyen la piratería de las cuentas de correo electrónico de miembros del personal, el envío de correos electrónicos de suplantación de identidad para obtener los datos de las cuentas de los miembros del personal y la explotación de los proveedores de comunicaciones para suplantar nombres de dominio que resulten familiares a la organización objetivo[186]. Los delincuentes adoptan diversas narrativas, como explotar una relación existente entre dos empresas mediante la emisión de una factura falsa, enviar un correo electrónico haciéndose pasar por un alto funcionario que presenta una solicitud urgente de fondos y hacerse pasar por un abogado que solicita una transferencia bancaria para tratar un asunto delicado[187]. La comunicación puede producirse durante un período de tiempo y los delincuentes pueden invertir tiempo en comprender la organización y sus sistemas a fin de defraudarla en múltiples ocasiones (véanse los estudios de casos que se presentan más adelante).

Fraude de choque por dinero

El fraude de choque por dinero implica a grupos delictivos que defraudan sistemáticamente a aseguradoras de vehículos[188]. Se utilizan diversos métodos, como la presentación de informes falsos de accidentes para reclamar el dinero del seguro y, en casos más graves, provocar accidentes de tráfico en los que se ven implicados ciudadanos inocentes para reclamar dinero de su seguro[189].

[185] INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas".

[186] Norah S. Al-Musib *et al.*, "Business email compromise (BEC) attacks", *Materials Today: Proceedings* (vol. 81, parte 2 (2023); y Geoffrey Simpson, Tyler Moore y Richard Clayton, "Ten years of attacks on companies using visual impersonation of domain names", en *2020 Anti-Phishing Working Group (APWG) Symposium on Electronic Crime Research (eCrime)* (Boston (Estados Unidos), 2020).

[187] Alessandro E. Agazzi, "Business email compromise (BEC) and cyberpsychology" (2020).

[188] Mark Button *et al.*, "Just about everybody doing the business? Explaining 'cash-for-crash' insurance fraud in the United Kingdom", *The Australian and New Zealand Journal of Criminology*, vol. 50, núm. 2 (junio de 2017).

[189] Mark Button y Graham Brooks, "From 'shallow' to 'deep' policing: 'crash-for-cash' insurance fraud investigation in England and Wales and the need for greater regulation", *Policing and Society*, vol. 26, núm. 2 (2016).

ESTUDIO DE CASO: VULNERACIÓN DEL CORREO ELECTRÓNICO EMPRESARIAL

Un fraude cometido mediante la vulneración del correo electrónico de una empresa de los Estados Unidos de América le hizo perder 1 millón de dólares. Los autores eran un grupo de tres coautores, dos de los cuales se encontraban en Nigeria. Los delincuentes se hicieron pasar por otra empresa con sede en los Estados Unidos con la que la víctima mantenía una relación comercial. Enviaron un primer correo electrónico solicitando el pago de los servicios que la empresa había prestado y un segundo correo electrónico solicitando que el dinero se enviara a una cuenta bancaria distinta, supuestamente por motivos fiscales. La cuenta bancaria era propiedad de una persona situada en otro país. Se cree que los beneficios se repartieron entre los tres codelincuentes.

Fuente: Unidad de Inteligencia Financiera de Nigeria, "Nigeria releases money-laundering typologies through fraud report", 12 de agosto de 2023.

ESTUDIO DE CASO: VULNERACIÓN DEL CORREO ELECTRÓNICO EMPRESARIAL

Los delincuentes enviaron un correo electrónico de suplantación de identidad al director financiero de una empresa que parecía proporcionar un enlace a la página de inicio de sesión del servicio de tecnologías de la información y las comunicaciones de la empresa. Al hacer clic en el enlace, la víctima era conducida a una página web que se parecía a la legítima. El funcionario de finanzas introdujo sus credenciales de acceso, que fueron capturadas por los delincuentes y utilizadas para acceder a su cuenta de correo electrónico. A continuación, lograron hacerse pasar por la víctima y enviar correos electrónicos a otros miembros del equipo financiero, solicitando una serie de transferencias bancarias a cuentas bajo su control. Además, observaron las políticas y prácticas de la empresa para aprender de ellas y lograron imitar un correo electrónico y una factura que se recibirían normalmente de un proveedor legítimo. Las facturas falsas se abonaban en cuentas controladas por los delincuentes. La empresa sufrió pérdidas financieras de aproximadamente 11 millones de dólares.

Fuente: United States of America v. Okeke, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

El fraude es un fenómeno muy diverso, que abarca una enorme variedad de métodos y técnicas para emplear el engaño con el fin de obtener un beneficio ilícito. Además, los métodos utilizados por quienes cometen fraude evolucionan continuamente para aprovechar las oportunidades de delinquir que surgen de los avances en las comunicaciones, el comercio, las finanzas y la tecnología. Agrupar los diversos métodos en un marco único para comprender el problema es un reto considerable, pero esencial para el desarrollo de políticas públicas amplias y cohesionadas dirigidas a hacer frente al fraude organizado. Esta tipología constituye un paso importante en el desarrollo de un marco para conceptualizar este delito polifacético.

CAPÍTULO III

Delincuentes implicados en el fraude organizado

Los delincuentes implicados en el fraude organizado poseen diferentes características y siguen distintas vías para delinquir. Esta diversidad tiene su origen en el amplio abanico de métodos (y capacidades necesarias) que se utilizan para perpetrar el fraude, la variedad de entornos en los que puede surgir, incluidos los diferentes entornos sociales, económicos y políticos de las distintas regiones del mundo, y la diversidad de funciones que cumplen y motivaciones que los impulsan. Es importante comprender quién comete el fraude organizado y las vías que se siguen para perpetrar este tipo de delitos a fin de orientar las intervenciones que resulten eficaces para disuadir y apartar a las personas de su comisión.

Los autores de delitos de fraude constituyen una población oculta y de difícil acceso, y la investigación sobre ellos sigue desarrollándose. La presente sección contiene una recopilación de pruebas para debatir, en primer lugar, la importancia de la coautoría; en segundo lugar, las características de los delincuentes organizados que cometen fraude, y, en tercer lugar, las motivaciones para perpetrar estos delitos.

Función e importancia de la coautoría de delitos

Los caminos que llevan a la delincuencia organizada vienen determinados en parte por las oportunidades de delinquir que surgen de las actividades cotidianas y de proximidad, los entornos y las relaciones de confianza (p. ej., las redes sociales y profesionales)[190]. La capacidad de reunirse y forjar relaciones de confianza con personas afines puede aumentar las posibilidades de delinquir de formas que de otro modo estarían fuera de alcance[191]. Esto incluye a los coautores que tienen recursos o capacidades de disponibilidad más limitada (p. ej., facilitadores profesionales o ciberdelincuentes con conocimientos técnicos)[192] y otros con capacidades más generalizadas (p. ej., operadores de centros de llamadas o mulas de dinero). Determinar los recursos y capacidades que se necesitan para perpetrar distintos tipos de fraude puede ayudar a identificar a los grupos vulnerables a ser arrastrados por la delincuencia

[190] Edward R. Kleemans y Henk G. van de Bunt, "Organised crime, occupations and opportunity", *Global Crime*, vol. 9, núm. 3 (2008); Edward R. Kleemans y Henk G. van de Bunt, "The social embeddedness of organized crime", *Transnational Organized Crime*, vol. 5, núm. 1 (1999); y Markus Felson, *The Ecosystem for Organized Crime*, Instituto Europeo de Prevención del Delito y Lucha contra la Delincuencia, afiliado a las Naciones Unidas, documento núm. 26 (Helsinki, 2006).

[191] Edward R. Kleemans y Christianne J. de Poot, "Criminal careers in organized crime and social opportunity structure", *European Journal of Criminology*, vol. 5, núm. 1 (enero de 2008).

[192] Jason R. C. Nurse y Maria Bada, "The group element of cybercrime: types, dynamics, and criminal operations", en *The Oxford Handbook of Cyberpsychology*, Alison Attrill-Smith *et al.*, eds. (Oxford, Oxford University Press, 2019).

organizada; como ejemplos, cabe mencionar la posibilidad de que los profesionales del derecho sean corrompidos y de que los estudiantes sean reclutados como mulas de dinero[193].

Los lugares en los que pueden coincidir los posibles coautores son importantes, porque sin esos puntos de convergencia es menos probable que se reúnan y que se produzcan los actos de delincuencia organizada. La disponibilidad y accesibilidad de estos puntos de convergencia es importante para determinar quién se involucra en la delincuencia organizada y cómo esta toma forma[194]. En el contexto del ciberfraude se destaca especialmente el crecimiento de las comunicaciones en línea tanto en la red abierta como en la web oscura, que ofrecen espacios para que los delincuentes coincidan, se comuniquen y comercien con otros delincuentes (véase el estudio de caso que se presenta más adelante). Los mercados y foros delictivos en línea, que ofrecen a los delincuentes (incluidos los que cometen fraude) un lugar donde intercambiar recursos y conocimientos, son un ejemplo clave de ello[195]. De estos entornos ha surgido el modelo de delincuencia como servicio, una economía subterránea en la que los empresarios de la ciberdelincuencia pueden beneficiarse del suministro de herramientas técnicas, recursos y servicios a quienes cometen fraude (y a otros delincuentes)[196]. Entre los principales productos y servicios que se pueden comprar o alquilar figuran datos personales robados, servicios de suplantación de identidad y correo electrónico no deseado, servicios de blanqueo de dinero (incluidas mulas de dinero), piratería de cuentas y el suministro de redes de bots[197].

La tecnología ha creado nuevas oportunidades para que quienes desean perpetrar actos de fraude formen grupos delictivos organizados a partir de una reserva mundial de posibles coautores[198]. Además, constituye una puerta de entrada a la actuación delictiva conjunta y a la delincuencia organizada accesible a quienes desean cometer actos de fraude. El anonimato de los espacios en línea mitiga los riesgos que conlleva cooperar con actores desconocidos, y los nuevos miembros pueden establecerse rápidamente y crearse una reputación en estas comunidades en línea[199]. Las alianzas pueden ser efímeras y existir únicamente para facilitar la realización de una tarea concreta, o bien estas nuevas tecnologías pueden fomentar una colaboración más duradera.

Las relaciones formadas fuera de Internet siguen siendo una característica clave de los grupos delictivos organizados que se dedican al ciberfraude y a menudo representan los elementos más estables y duraderos de un grupo[200]. Esto incluye a los grupos delictivos organizados que amplían su repertorio delictivo para incluir el fraude, o a los asociados que se reúnen con el propósito de cometer fraude. Estos grupos pueden pasar a ser híbridos integrándose en la economía subterránea en línea para acceder a recursos delictivos y a coautores[201]. El fraude organizado implica la utilización de métodos complejos de delinquir, que suelen incluir una larga secuencia de acciones y acontecimientos que a menudo están separados entre sí en el tiempo y el espacio[202], lo que a su vez puede atenuar las relaciones

[193] Australia, Transaction Reports and Analysis Centre, "Combating the exploitation of international students as money mules: financial crime guide" (2024); y May y Bhardwa, *Organised Crime Groups Involved in Fraud*.

[194] Felson, *The Ecosystem for Organized Crime*; y Kleemans y de Poot, "Criminal careers in organized crime".

[195] Soudijn y Zegers, "Cybercrime and virtual offender convergence settings"; y Yip, Webber y Shadbolt, "Trust among cybercriminals?".

[196] INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 11.

[197] Akyazi, van Eeten y Gañán, "Measuring cybercrime as a service (CaaS)"; An y Kim, "A data analytics approach"; Jirovsky *et al.*, "Cybercrime and organized crime"; e INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 11.

[198] Soudijn y Zegers, "Cybercrime and virtual offender convergence settings".

[199] Odinot *et al.*, Organised Cybercrime in the Netherlands; y Yip, Shadbolt y Webber, "Why forums?".

[200] Leukfeldt, Lavorgna y Kleemans, "Organised cybercrime or cybercrime that is organized?"; Lusthaus *et al.*, "Cybercriminal networks in the United Kingdom and beyond"; y Odinot *et al.*, *Organised Cybercrime in the Netherlands*.

[201] Roderic Broadhurst *et al.*, "Crime in cyberspace: offenders and the role of organized criminal groups", documento de trabajo (Canberra, Australian National University Cybercrime Observatory, 2013); y Choo, "Organized crime groups in cyberspace".

[202] Klaus von Lampe, "Situational prevention of 'organised crime': preventing phantom conceptions with phantom means?", en *Cross-border Crime Inroads on Integrity in Europe*, Petrus C. van Duyne *et al.*, eds. (Nimega (Reino de los Países Bajos), Wolf Legal Publishers, 2010).

entre los distintos delincuentes situados a lo largo de esa secuencia[203]. El resultado es que las tareas se distribuyen entre una multitud de actores delictivos que no están estrechamente vinculados entre sí, lo que aumenta su capacidad para especializarse y acumular conocimientos específicos. Además, una distribución más uniforme de las tareas y funciones entre los miembros de un grupo delictivo organizado sirve para repartir la culpabilidad y el riesgo de detección por parte de las entidades encargadas de hacer cumplir la ley.

ESTUDIO DE CASO: MERCADO DELICTIVO

Genesis Market ofrecía a los delincuentes un punto de encuentro en línea para comerciar con identidades digitales. El mercado ofrecía a la venta bots que habían infectado los dispositivos de diversas víctimas mediante programas maliciosos o un ataque de apropiación de cuentas. El precio de cada bot dependía de la cantidad y calidad de los datos recopilados (los más valiosos eran los datos de acceso a cuentas bancarias en línea). Los delincuentes que compraban los bots recibían los datos y un *software* capaz de seguir las huellas dejadas en el navegador, que les permitía imitar el comportamiento de las víctimas al acceder a la cuenta y eludir las medidas de seguridad antifraude de la plataforma. Accedieron al mercado delincuentes de todo el mundo y se calcula que se habían alojado en el sitio 80 millones de credenciales robadas a 2 millones de personas.

Fuente: Agencia de la Unión Europea para la Cooperación Policial (Europol), "Takedown of notorious hacker marketplace selling your identity to criminals", 5 de abril de 2023.

ESTUDIO DE CASO: LA DELINCUENCIA COMO SERVICIO

Un sitio web delictivo suministraba el programa informático iSpoof, que habilitaba a los delincuentes a realizar llamadas telefónicas que parecían proceder de entidades de confianza, como bancos, empresas de venta al por menor e instituciones gubernamentales. Esto permitía a los delincuentes hacerse pasar por organizaciones legítimas de forma más creíble cuando se ponían en contacto con las víctimas, facilitando así el engaño. El sitio web se comercializaba entre los delincuentes a través de la aplicación de mensajería cifrada Telegram y llegó a tener hasta 59.000 usuarios en todo el mundo que pagaban una cuota mensual para acceder a sus servicios. Había varios administradores, pero una persona residente en el Reino Unido de Gran Bretaña e Irlanda del Norte había desempeñado un papel destacado en la creación del programa informático y la administración del sitio web. A lo largo de 16 meses, el sitio web ganó más de 3,7 millones de euros y gran parte de esas ganancias fueron a parar al administrador principal.

Fuentes: Agencia de la Unión Europea para la Cooperación Policial (Europol), "Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests", 24 de noviembre de 2022; y "Fraudster jailed for running multimillion-pound website iSpoof", *The Guardian*, 19 de mayo de 2023.

[203] Por ejemplo, la falsificación de identidad requiere el robo de datos personales, la creación de un foro en línea en el que vender la información, la adquisición de los datos por parte de quienes cometen fraude, la selección y compra de productos y servicios en una plataforma, el reclutamiento de mulas para recibir los objetos robados y la reventa de esos objetos con fines de lucro (Bodker *et al.*, "Card-not-present fraud").

Características de quienes cometen delitos de fraude organizado

No existe un perfil típico de persona que comete fraude. A medida que se amplían las oportunidades de delinquir, especialmente en el contexto del ciberfraude, siguen diversificándose las vías y los perfiles en todo el mundo. Los distintos métodos para cometer fraude surgen en diferentes entornos sociales, comerciales, financieros y tecnológicos, cada uno de los cuales requiere recursos o capacidades particulares, lo que significa que las vías y características de quienes cometen fraude también pueden ser diferentes dentro de la multitud de entornos.

Históricamente, la mayor parte del fraude se ha cometido desde entornos de cuello blanco. En este contexto, los autores suelen ser personas por otra parte respetuosas de la ley que deciden explotar las oportunidades que surgen en un entorno laboral legítimo, por ejemplo, malversación, quiebra o fraude fiscal[204]. En el contexto de la delincuencia organizada, los autores de fraudes de cuello blanco normalmente han tenido poco contacto con los sistemas de justicia penal antes de su condena por fraude organizado y tienden a ser mayores que otras personas implicadas en la delincuencia organizada[205]. Es probable que esto se deba a que las oportunidades de cometer fraude de cuello blanco están más restringidas a las personas que ejercen profesiones legítimas establecidas y son capaces de cruzar los delgados márgenes que separan las prácticas lícitas de las ilícitas[206]. Quienes cometen fraude de cuello blanco siguen representando un elemento significativo del problema del fraude organizado (véase la sección sobre fraude contra empresas u organizaciones en el capítulo II); sin embargo, las pruebas indican una diversidad mucho mayor en las vías de acceso al fraude organizado y en las características de los autores. También es importante reconocer la participación tanto de hombres como de mujeres en el fraude organizado. Debido a los estereotipos relacionados con la delincuencia organizada imperantes, las mujeres son vistas predominantemente como víctimas y rara vez como autoras. Sin embargo, las investigaciones han indicado que la realidad es más compleja y que hombres y mujeres pueden ser tanto autores como víctimas del fraude organizado[207].

Las conceptualizaciones de los delitos de cuello blanco se han arraigado menos en determinadas categorías de delincuentes (p. ej., los de clase alta) y se han centrado en cambio en ciertos tipos de delitos que implican la vulneración de la confianza[208]. Existen muchos tipos de fraude organizado en los que se crea (o se llega a utilizar) una empresa con el único fin de cometer fraude. Una empresa proporciona una fachada legítima para facilitar el engaño a las víctimas y a las autoridades; algunos ejemplos destacados son los centros de llamadas para relacionarse con el público y las empresas comerciales creadas para vender productos o servicios fraudulentos o facilitar el blanqueo de dinero[209]. Esto puede implicar el establecimiento de una plantilla asalariada con una división del trabajo perfectamente

[204] Victor R. van der Geest, David Weisburd y Arjan A. J. Blokland, "Developmental trajectories of offenders convicted of fraud: a follow-up to age 50 in a Dutch conviction cohort", *European Journal of Criminology*, vol. 14, núm. 5 (septiembre de 2017). Cabe señalar que el presente documento temático no abarca el fraude fiscal.

[205] Un estudio realizado en el Reino Unido reveló que la edad media de las personas identificadas por las entidades encargadas de hacer cumplir la ley de ese país como participantes en actos de fraude organizado era de 41 años (May y Bhardwa, *Organised Crime Groups Involved in Fraud*, pág. 113. Véanse también Russell G. Smith, "Responding to organised crime through intervention in recruitment pathways", Trends and Issues in Crime and Criminal Justice Series, núm. 473 (Canberra, Instituto Australiano de Criminología, 2014); y M. Vere van Koppen *et al.*, "Criminal trajectories in organized crime", *The British Journal of Criminology*, vol. 50, núm. 1 (enero de 2010)).

[206] Van Koppen *et al.*, "Criminal trajectories in organized crime".

[207] UNODC, *Organized Crime and Gender: Issues Relating to the United Nations Convention against Transnational Organized Crime* (Viena, 2022).

[208] Anna Gekoski, Joanna Ruth Adler y Tim McSweeney, "Profiling the fraudster: findings from a rapid evidence assessment", *Global Crime*, vol. 23, núm. 4 (2022); y David O. Friedrichs, *Trusted Criminals: White Collar Crime in Contemporary Society*, 4ª ed. (Belmont (California, Estados Unidos), Wadsworth, 2010).

[209] Véase, por ejemplo, Miramirkhani, Starov y Nikiforakis, "Dial one for scam"; Shover, Coffey y Sanders, "Dialing for dollars"; y UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia*.

definida y que imite de hecho las estructuras de empresas legales. Las empresas pueden operar al descubierto, camufladas dentro de sectores legítimos, y en algunos casos pueden ocupar zonas grises que se encuentran en la periferia de las prácticas empresariales o comerciales reguladas (véase el estudio de caso que se presenta más adelante).

La ciberdelincuencia ha dado lugar a la diversificación de las características de los autores de fraudes. La tecnología está cambiando las nociones tradicionales de "delincuencia callejera", con tecnologías cada vez más accesibles que crean oportunidades para que los delincuentes se dediquen a actividades delictivas como la suplantación de identidad y el fraude en línea[210]. Muchos casos de ciberfraude se cometen desde fuera de entornos comerciales legítimos o pseudolegítimos, a menudo empleando la tecnología para hacerse pasar por una entidad con la que la víctima tiene una relación legítima[211]. La tecnología proporciona la puerta de entrada para la participación en estos delitos, que pueden implicar múltiples formas de ciberdelincuencia (p. ej., ataques con programas secuestradores), lo que significa que es posible que las nociones tradicionales de autor de fraude ya no representen a los delincuentes capaces de participar en diversos ciberdelitos con el fin de obtener beneficios financieros[212]. Esta diversificación se ve facilitada en parte por la disponibilidad cada vez más generalizada de recursos de conocimiento tecnológico a través de redes delictivas en línea que pueden servir para ampliar las capacidades de un grupo delictivo organizado[213].

Esta expansión de las oportunidades de delinquir es evidente en muchos países y regiones. Diversos estudios han puesto de relieve un fenómeno en el que las diversas metodologías específicas para cometer fraude se concentran en determinadas regiones del mundo[214]. Algunos ejemplos clave son la concentración de fraudes románticos, de inversión y otros fraudes de publicidad masiva de gran impacto perpetrados en África Occidental y fuertemente asociados a la cultura juvenil local[215]; fraudes de lotería dirigidos a los Estados Unidos pero que emanan de Jamaica[216]; "centros de ciberdelincuencia" situados geográficamente en Europa Oriental que se dedican a fraudes como el de las subastas en línea, en los que los implicados comparten recursos y aprendizaje[217]; y los complejos desde donde se realizan estafas en Asia Sudoriental, que han industrializado procesos para perpetrar fraudes románticos y de inversión en criptomonedas[218].

---

[210] Leukfeldt, "Cybercrime and social ties"; y Robert A. Roks, Eric Rutger Leukfeldt y James A. Densley, "The hybridization of street offending in the Netherlands", *The British Journal of Criminology*, vol. 61, núm. 4 (julio de 2021).

[211] Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[212] A modo de ejemplo, se ha informado de que grupos delictivos organizados dedicados al ciberfraude en Asia Sudoriental han diversificado su modelo de negocio e incluyen el desarrollo de programas maliciosos o aplicaciones móviles o web maliciosas y la prestación de diversos ciberdelitos como servicio (UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia*).

[213] A modo de ejemplo, un grupo delictivo organizado del Reino Unido había estado implicado en múltiples categorías de ciberfraude (falsificación de identidad y fraude de vulneración del correo electrónico empresarial). También se especializaba en facilitar el blanqueo de dinero y participó en un ataque con programas secuestradores contra empresas locales. Los principales delincuentes no tenían conocimientos técnicos, pero podían acceder a recursos técnicos de otros delincuentes, también en línea, como en los foros de *carding* (comercio de tarjetas) (Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending", pág. 30).

[214] INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 11.

[215] Suleman Ibrahim, "Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals", *International Journal of Law, Crime and Justice*, vol. 47 (2016); y Monica T. Whitty, "419: it's just a game – pathways to cyber-fraud", *International Journal of Cyber Criminology*, vol. 12, núm. 1 (enero/junio de 2018).

[216] Mortley, "A crime of opportunity".

[217] Jonathan Lusthaus y Federico Varese, "Offline and local: the hidden face of cybercrime", *Policing: A Journal of Policy and Practice*, vol. 15, núm. 1 (marzo de 2017).

[218] UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*.

ESTUDIO DE CASO: DELITOS DE CUELLO BLANCO – FRAUDE EN LAS INVERSIONES

En el Reino Unido de Gran Bretaña e Irlanda del Norte, unos delincuentes crearon una empresa con el fin de defraudar a los titulares de pensiones para despojarlos de sus ahorros. Adquirieron un estatus regulado para aparecer como un proveedor legítimo y procedieron a comercializar sus servicios financieros realizando llamadas no solicitadas al público. Conocían y comprendían en detalle el sector de las pensiones en el Reino Unido, las leyes y reglamentos pertinentes, las inversiones y otros instrumentos financieros. Con estos conocimientos, los delincuentes pudieron aprovecharse de las considerables lagunas del público. Empleaban un engaño de varios niveles que consistía, en primer lugar, en transmitir a las víctimas información falsa sobre sus obligaciones fiscales para animarlas a soltar dinero. El dinero pasaba entonces por las manos de múltiples coautores, que desempeñaban el papel de intermediarios financieros y cobraban comisiones desmesuradamente altas por tramitar la transferencia de fondos. El dinero restante presuntamente se invertía en una empresa extranjera legítima pero de alto riesgo. El dinero o bien se perdía tras el fracaso de la inversión o bien podía que nunca se invirtiera, sino que fuera robado por los delincuentes.

Fuente: Michael Skidmore, *Protecting People's Pensions: Understanding and Preventing Scams* (Londres, The Police Foundation, 2020), pág. 15.

Motivaciones de los autores de fraude

La tecnología ha "democratizado" la comisión de delitos de fraude al generar oportunidades de delinquir para personas de cualquier estrato social, incluidas las procedentes de entornos pobres y desfavorecidos, que no requieren funciones profesionales específicas ni aptitudes y conocimientos afines para poder perpetrar un fraude organizado[219]. Esta delincuencia puede estar arraigada en subculturas locales, en las que se propagan actitudes criminógenas, conocimientos especializados y metodologías[220]. En algunos contextos, el ciberfraude goza de legitimidad social, con racionalizaciones o actitudes particulares compartidas por los miembros de una comunidad o grupo, y quienes logran cometer fraudes gozan de un estatus social elevado[221].

La obtención de un beneficio del delito (de índole financiera u otro beneficio material) es la motivación clave en el fraude, como en prácticamente cualquier delito adquisitivo, lo que puede ser la respuesta a una situación financiera adversa, como la ausencia de oportunidades legítimas y la privación[222]. En Nigeria, muchas de las personas que cometen ciberfraude son estudiantes o graduados universitarios, por lo general de entre 20 y 30 años de edad, con conocimientos avanzados y aptitudes en el ámbito de la tecnología[223]. La brecha entre los crecientes niveles de formación y educación y las perspectivas en la economía legal puede hacer que, para ganarse la vida, las personas recurran a salidas ilegítimas

[219] Van der Geest, Weisburd y Blokland, "Developmental trajectories of offenders convicted of fraud"; y Wall, "Dis-organised crime".

[220] Véanse, por ejemplo, Alice Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission", *Crime, Law and Social Change*, vol. 62, núm. 1 (agosto de 2014); Lusthaus y Varese, "Offline and local"; Jegede Ajibade Ebenezer, "Cyber fraud, global trade and youth crime burden: Nigerian experience", *Afro Asian Journal of Social Sciences*, vol. 5, núm. 4 (2014); y Ojedokun e Ilori, "Tools, techniques and underground networks".

[221] Shover, Coffey y Sanders, "Dialing for dollars"; Whitty, "419: it's just a game"; y Oludayo Tade e Ibrahim Aliyu, "Social organization of Internet fraud among university undergraduates in Nigeria", *International Journal of Cyber Criminology*, vol. 5, núm. 2 (julio/diciembre de 2011).

[222] Mortley, "A crime of opportunity".

[223] Aransiola y Asindemade, "Understanding cybercrime perpetrators"; y Tade y Aliyu, "Social organization of internet fraud".

como el ciberfraude[224]. Se ha observado un patrón similar entre las personas reclutadas para trabajar en compuestos dedicados a las estafas en Asia Sudoriental: los grupos delictivos organizados reclutan a miles de trabajadores, muchos de los cuales tienen entre 20 y 30 años de edad y son graduados universitarios con conocimientos de tecnologías de la información y las comunicaciones, redes sociales, criptomonedas e idiomas[225]. Muchos solicitan estos puestos por falta de oportunidades de trabajo legítimas, aunque, lo que es importante, muchos son engañados para aceptar lo que se presenta como un puesto legítimo antes de ser víctimas de la trata y coaccionados para cometer fraudes[226].

Los delincuentes que se involucran en grupos delictivos organizados pueden tomar la decisión consciente e intencionada de participar en el fraude o pueden ser reclutados por un grupo delictivo organizado sin haber tenido ninguna intención previa de implicarse en la delincuencia organizada[227]. En el caso de los que toman una decisión intencionada, pueden haber sido motivados por varias razones, como la codicia al ver una oportunidad de ganar dinero rápido, la influencia de pares o asociados en un grupo delictivo organizado existente u otro grupo (fuera de línea o en línea), o una situación de necesidad o dificultad financiera[228].

Entre las personas que no tenían una intención previa de implicarse, muchos son reclutados por grupos delictivos organizados para desempeñar funciones de facilitación periféricas, pero importantes. Puede tratarse de personas reclutadas por poseer conocimientos técnicos especializados adquiridos en el ejercicio de una profesión determinada que puede facilitar alguna parte del proceso penal (p. ej., abogados o contables), jóvenes profesionales reclutados como "mano de obra" y miembros del público reclutados para desempeñar funciones como la de mula de dinero. El grado de conocimiento y complicidad entre estos individuos puede ser diferente y cambiar con el tiempo: algunos no son conscientes del propósito fraudulento subyacente de la actividad, otros se contentan con aceptar el dinero sin hacer demasiadas preguntas y otros llegan a participar en el delito a sabiendas[229]. Algunos coautores de fraude son explotados por el grupo delictivo organizado; suelen ser los más expuestos a la detección por parte de las fuerzas de seguridad y, por tanto, sirven para poner distancia entre los delincuentes principales y el fraude, y en algunos casos reciben poco o ningún beneficio económico por su participación[230]. En Asia Sudoriental, un ejemplo reciente y conmovedor es el de algunos jóvenes que aceptaron trabajar en complejos dedicados a las estafas y luego fueron objeto de trata de personas y explotación[231].

Una última cuestión que cabe tener en cuenta es cómo llegan los autores de fraude a tomar la decisión de atacar a las víctimas y robarles dinero, teniendo en cuenta que, de otro modo, algunos podrían no

---

[224] Akanle, Adesina y Akarah, "Towards human dignity and the internet"; y Suleman Lazarus y Geoffrey U. Okolorie, "The bifurcation of the Nigerian cybercriminals: narratives of the Economic and Financial Crimes Commission (EFCC) agents", *Telematics and Informatics*, vol. 40 (2019).

[225] Organización Internacional para las Migraciones (OIM), Oficina Regional para Asia y el Pacífico, "IOM's regional situation report on trafficking in persons into forced criminality in online scamming centre in Southeast Asia" (2024); UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*.

[226] ACNUDH, "Online scam operations and trafficking into forced criminality in Southeast Asia".

[227] Smith, "Responding to organised crime through intervention in recruitment pathways".

[228] Véanse, por ejemplo, W. Steve Albrecht y Chad O. Albrecht, *Fraud Examination and Prevention* (Mason (Ohio, Estados Unidos), Thompson South-Western, 2004); Hutchings, "Crime from the keyboard"; Yetunde O. Ogunleye, Usman A. Ojedokun y Adeyinka A. Aderinto, "Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in South-West Nigeria", *International Journal of Cyber Criminology,* vol. 13, núm. 2 (julio/diciembre de 2019); y May y Bhardwa, *Organised Crime Groups Involved in Fraud*.

[229] Shover, Coffey y Sanders, "Dialing for dollars"; Leukfeldt y Jansen, "Cyber criminal networks and money mules"; Levi, "Organized fraud and organizing frauds"; Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending"; y May y Bhardwa, *Organised Crime Groups Involved in Fraud*.

[230] Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[231] UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*.

dedicarse a la delincuencia[232]. El proceso de racionalización para justificar o neutralizar el impacto del delito es importante, porque puede distorsionar las narrativas personales o de grupo sobre la gravedad de las acciones o incluso servir para legitimarlas. Entre los ejemplos clave cabe mencionar lo siguiente:

- La percepción de una relación de confrontación con las víctimas. Un estafador que tiene éxito demuestra habilidad, dominio y poder para controlar y manipular a las víctimas, que pueden ser consideradas indignas (p. ej., estúpidas o codiciosas) y culpadas por caer en el fraude[233].
- La percepción de que el delito no tiene víctimas o causa un daño mínimo. Esta percepción puede darse, por ejemplo, cuando los autores emplean un método que implica el robo de pequeñas cantidades de dinero a un elevado número de personas o cuando las víctimas son sociedades comerciales y empresas en lugar de particulares[234].
- La naturaleza anónima y remota del fraude, que consiste en intercambios impersonales que no implican contacto cara a cara con la víctima. Los delincuentes no observan entonces directamente el daño que causan, lo que puede permitirles neutralizar más fácilmente sus delitos[235]. Además, en el contexto de la ciberdelincuencia, la capacidad de permanecer físicamente invisible, de separar la acción en línea de la identidad fuera de línea y de percibir el mundo en línea como no conectado con la "realidad" quita inhibiciones a quienes, de otro modo, no cometerían delitos[236].
- Las influencias sociales y culturales que pueden servir para racionalizar el fraude. Estas influencias pueden incluir narrativas sociopolíticas y percepciones respecto de las víctimas que se encuentran en el extranjero: algunos autores legitiman sus acciones basándose en ideas de desigualdades o injusticias sociales actuales o históricas (p. ej., "occidentales codiciosos")[237]. En algunas culturas, la comisión de fraudes puede incluso verse reforzada por las creencias espirituales locales[238].

Las modalidades de los delitos de fraude han experimentado cambios sustanciales en los últimos 10 a 20 años y siguen evolucionando a gran velocidad. La investigación y la base de conocimientos en la materia siguen desarrollándose y actualizándose en función de esos cambios. Las características de los delincuentes y sus vías de acceso al fraude organizado son muy variables, pero hay pautas de comportamiento que han empezado a surgir en las distintas regiones del mundo y en los diferentes entornos comerciales, financieros y tecnológicos que propician las oportunidades de delinquir. Comprender quiénes son estos delincuentes y sus vías de acceso al fraude organizado es un paso importante para formular políticas sociales y de justicia penal eficaces que aborden estos comportamientos delictivos.

---

[232] Por ejemplo, el "triángulo del fraude" es una teoría destacada para explicar la delincuencia de cuello blanco. Define tres condiciones para que un delincuente cometa fraude: a) un incentivo o presión que proporcione un motivo para cometer fraude; b) una oportunidad para cometer fraude, y c) una actitud que permite al individuo cometer el fraude o tener la capacidad de racionalizarlo (véase Albrecht y Albrecht, *Fraud Examination and Prevention*).

[233] Duffield y Grabosky, *The Psychology of Fraud*; y Shover, Coffey y Sanders, "Dialing for dollars".

[234] Heath Copes y Lynne Vieraitis, "Identity theft: assessing offenders' motivations and strategies", en *In Their Own Words: Criminals on Crime*, 6ª ed., Michael L. Birzer y Paul Cromwell, eds. (Oxford (Reino Unido), Oxford University Press, 2014), págs. 124 a 139; Duffield y Grabosky, *The Psychology of Fraud*; y May y Bhardwa, *Organised Crime Groups Involved in Fraud*.

[235] Duffield y Grabosky, *The Psychology of Fraud*; y Alice Hutchings, "Cybercrime trajectories: an integrated theory of initiation, maintenance and desistance", en *Crime Online: Correlates, Causes, and Context*, Thomas J. Holt, ed. (Durham (Carolina del Norte, Estados Unidos), Carolina Academic Press, 2010).

[236] John Suler, "The online disinhibition effect", *Cyberpsychology and Behavior*, vol. 7, núm. 3 (2004).

[237] Mortley, "A crime of opportunity"; y Whitty, "419: it's just a game".

[238] En Nigeria, algunos creen que la adquisición de riqueza, ya sea por medios legítimos o ilegítimos, tiene sus raíces en el ámbito espiritual (Lazarus y Okolorie, "The bifurcation of the Nigerian cybercriminals").

CAPÍTULO IV

Facilitadores transversales del fraude organizado

Como se ha señalado en el capítulo II, son muy diversos los métodos empleados por los distintos delincuentes para estafar a las víctimas; sin embargo, los comportamientos y técnicas utilizados en diferentes tipos de fraude presentan algunas características comunes. Ello se debe a que, independientemente de la narrativa fraudulenta concreta que se presente a las víctimas, muchos tipos de fraude necesitan los mismos pasos generales, como establecer comunicación con las víctimas, utilizar métodos de comunicación que faciliten el engaño y acceder a los fondos robados sin dejar ningún rastro de pruebas[239]. La comprensión de los elementos comunes de la economía legítima e ilegítima explotados por los delincuentes permite adoptar nuevas estrategias e intervenciones de prevención del fraude organizado. En la presente sección se describen los siguientes recursos, técnicas y tecnologías básicos fundamentales que se han señalado en la bibliografía en materia de políticas e investigación: comercialización masiva, usurpación de identidad, blanqueo de dinero y funciones facilitadoras de la tecnología (incluidas las tecnologías emergentes como la inteligencia artificial).

Comercialización masiva

El éxito de muchos tipos de fraude relacionados con el consumidor, el empleo y las inversiones depende de una comunicación eficaz en la que se utilizan distintas técnicas para persuadir a los posibles inversionistas. Entre ellas cabe citar las campañas dirigidas a destinatarios específicos o de comercialización masiva, técnicas de venta agresivas y la creación de recursos dirigidos a producir y mantener credibilidad y confianza, como la creación de una imagen de marca, sitios web y otros materiales de comercialización. Los delincuentes pueden emplear canales de comunicación específicos o una combinación de varios, los cuales utilizan en distintas etapas del delito. Por ejemplo, el contacto inicial con una víctima puede tener lugar mediante un sitio web de suplantación de identidad, seguido de una llamada telefónica de ventas y, posteriormente, un contacto continuado a través de un sitio web fraudulento (véase el estudio de caso que se presenta más adelante).

Telemarketing

Utilización de centros de llamadas o "salas de calderas" para llevar a cabo comercializaciones y ventas agresivas, a menudo en forma de llamadas no solicitadas a personas que se escogen utilizando "listas de

[239] En un informe se enuncian las siguientes tres etapas fundamentales del proceso de ciberfraude: a) la ruta de comunicación "de entrada"; b) la "interacción" con la víctima, y c) el "cobro" (Reino Unido, Cámara de los Lores, Ley Antifraude de 2006, y Digital Fraud Committee, *Fighting Fraud: Breaking the Chain*, Report of Session 2022-23, House of Lords Paper, núm. 87 (Londres, 2022)).

contactos" de posibles clientes ya sea elaboradas por otros agentes legítimos o ilegítimos que recopilan y venden esa información personal sobre los consumidores, o compradas a esos agentes[240]. En algunos casos, esas listas incluyen a personas que se sabe que ya han sido estafadas y que, por tanto, son potencialmente vulnerables a planteamientos similares; esto es un problema especialmente grave en el caso de las víctimas de edad avanzada en contextos de vulnerabilidad[241]. Los centros de llamadas pueden ser gestionados directamente por los delincuentes que dirigen el plan fraudulento o contratados a especialistas capaces de prestar esos servicios de "sala de calderas". Dichos centros pueden estar situados en países distintos del de la víctima, a veces en jurisdicciones conocidas por tener controles menos estrictos sobre tales actividades[242].

Comunicaciones en línea

Ha habido un aumento sustancial del tipo de fraude en que el contacto inicial con las víctimas se establece a través de comunicaciones en línea, como los medios sociales y sitios web y aplicaciones fraudulentos[243]. La accesibilidad de las tecnologías digitales y los grandes conjuntos de datos sobre los consumidores aumentan enormemente la capacidad de realizar una comercialización selectiva y en gran escala. Por ejemplo, pueden utilizarse sitios web y la publicidad en línea para recopilar datos sobre las personas que muestran interés en el producto o el servicio ofrecidos, lo que permite focalizar la comunicación posterior[244].

Otras comunicaciones

Otros métodos de fraude consisten en la comercialización a través del servicio postal o en persona[245]. Algunas categorías, como el fraude en las inversiones, a menudo implican grandes sumas de dinero que resultan muy considerables para las víctimas, mientras que en algunos casos el contacto cara a cara sigue siendo importante para lograr niveles de confianza suficientes para lograr una inversión. Algunos estafadores eligen víctimas con las que tienen conexiones sociales o comerciales para explotar una relación de confianza ya existente[246].

Usurpación de identidad

En una sociedad de la información en que las operaciones digitales sustituyen cada vez más la interacción presencial, resultan decisivos los instrumentos y mecanismos de verificación de la identidad[247]. La usurpación de identidad y la falsificación de identidad representan dos actividades diferenciadas: la usurpación de identidad se refiere a los procesos de acceso a los datos y el robo de estos, mientras que la falsificación de identidad consiste en utilizar los datos robados para engañar a las víctimas y acceder de manera fraudulenta a fondos u otros beneficios materiales. Las tecnologías de la información y las comunicaciones y los macrodatos facilitan la transferencia de información a una escala sin precedentes, y esa es una capacidad que explotan los delincuentes. La tecnología se comporta como un multiplicador

[240] Shover, Coffey y Sanders, "Dialing for dollars"; Levi, "Organized fraud and organizing frauds"; y Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[241] Age UK, *Only the Tip of the Iceberg: Fraud against Older People Evidence Review* (Londres, 2015); y Mark Button *et al.*, "Fear and phoning: telephones, fraud, and older adults in the UK", *International Review of Victimology* (2024).

[242] Shover, Coffey y Sanders, "Dialing for dollars".

[243] Véanse, por ejemplo, Estados Unidos, Buró Federal de Investigaciones, "The FBI warns of a spike in cryptocurrency investment schemes", 14 de marzo de 2023; y Reino Unido, Financial Conduct Authority, "FCA warns of increased risk of online investment fraud, as investors lose £87k a day to binary options scams", 2 de abril de 2024.

[244] Véase, por ejemplo, Liu *et al.*, "Understanding, measuring, and detecting".

[245] Véanse, por ejemplo, DeLiema y Langton, "Older victims of mass marketing scams"; y Phillips, "From 'rogue traders' to organized crime groups".

[246] Frank S. Perri y Richard G. Brody, "The optics of fraud: affiliations that enhance offender credibility", *Journal of Financial Crime*, vol. 19, núm. 3 (2012).

[247] Bert-Jaap Koops *et al.*, "A typology of identity-related crime", *Information Communication and Society*, vol. 12, núm. 1 (2009).

de fuerza para la usurpación de identidad, ya que aumenta la capacidad de acceder rápidamente a grandes volúmenes de información personal a nivel mundial[248]. Los métodos utilizados en la comisión de la usurpación de identidad comprenden los siguientes:

- Uso de técnicas de ingeniería social. Entre estas cabe citar los ataques de suplantación de identidad o *phishing*, de mensajes de SMS fraudulentos o *smishing* y de suplantación de identidad dirigida o *spear-phishing*[249], que utilizan comunicaciones orientadas a destinatarios específicos a fin de presionarlos para que adopten una decisión rápida y respondan (p. ej., una supuesta amenaza para la seguridad de una cuenta)[250]. Las campañas de suplantación de identidad constituyen una táctica de engaño para que una persona revele información personal y son una manera de atacar dispositivos electrónicos con programas maliciosos.
- Recopilación de datos de código abierto. Los delincuentes pueden sacar provecho de los datos que los usuarios publican en las plataformas de los medios sociales. A partir de programas informáticos automatizados, se pueden recopilar grandes volúmenes de datos, o un estafador puede elaborar el perfil de la víctima prevista para facilitar el engaño.
- Intrusión en una computadora o dispositivo o la infección de estos. Los estafadores infectan la computadora de la víctima con programas maliciosos que les permiten vigilar la actividad y recopilar detalles personales e información relativa a la cuenta. Uno de los métodos consiste en manipular el navegador de Internet de manera que, cuando la persona trate de acceder a un sitio web legítimo, sea dirigida hacia un sitio web falso que permite a los delincuentes recopilar información sobre la cuenta[251]. Las redes de bots y otros programas de vigilancia aumentan la capacidad de los atacantes para infectar un gran volumen de computadoras con programas maliciosos que el atacante puede controlar a distancia y utilizar para buscar información personal, como la de acceso a cuentas.
- Clonación digital de tarjetas. El empleo de programas maliciosos para infiltrarse en sitios web legítimos como los de los minoristas en línea se conoce como clonación digital de tarjetas o *digital skimming*. La información de pago (p. ej., las credenciales de las tarjetas de crédito) puede obtenerse o bien directamente de los formularios de pago legítimos o bien el comprador puede ser dirigido a una página web de cobro falsa para que proporcione sus datos[252].
- Violación de datos a través de la piratería informática u otros medios de intrusión en los sistemas de tecnologías de la información y las comunicaciones de las organizaciones que almacenan grandes volúmenes de datos personales[253]. El análisis de las violaciones de datos durante el período de 2005 a 2018 reveló que se habían producido 9.000 violaciones que dieron lugar a la pérdida de 11.500 millones de registros de datos, y que la piratería informática desempeñaba cada vez más un papel central[254]. El robo de datos personales de gran escala ofrece la posibilidad de diversos tipos de fraude, aunque se desconoce la proporción de los datos así utilizados.

---

[248] David S. Wall, "Policing identity crimes", *Policing and Society: An International Journal of Research and Policy*, vol. 23, núm. 4 (2013).

[249] La suplantación de identidad es una forma de comunicación que aparenta proceder de una fuente reputada y fiable y que está destinada a solicitar información personal o pagos o que puede contener archivos adjuntos que al abrirlos instalan programas maliciosos; los mensajes de SMS fraudulentos son una forma de suplantación de identidad que se valen de mensajes de texto o aplicaciones de mensajería; la suplantación de identidad dirigida consiste en un ataque más focalizado en que su autor utiliza información sobre el destinatario para que el mensaje resulte más realista y persuasivo. Véanse, por ejemplo, Europol, "Online fraude schemes"; y Europol, Centro Europeo contra la Ciberdelincuencia, "Spear phishing: a law enforcement and cross-industry perspective" (La Haya, 2019).

[250] Zainab Alkhalil *et al.*, "Phishing attacks: a recent comprehensive study and a new anatomy", *Frontiers in Computer Science*, vol. 3, art. núm. 563060 (marzo de 2021).

[251] Wall, "Policing identity crimes".

[252] Europol, "Online fraud schemes".

[253] Spencer Wheatley, Thomas Maillart y Didier Sornette, "The extreme risk of personal data breaches and the erosion of privacy", *The European Physical Journal B*, vol. 89, art. núm. 7 (enero de 2016).

[254] Hicham Hammouchi *et al.*, "Digging deeper into data breaches: an exploratory data analysis of hacking breaches over time", *Procedia Computer Science*, vol. 151 (2019).

La usurpación de identidad es un elemento vital que precede a muchos tipos de fraude y un facilitador clave de otros. Por ejemplo, facilita la falsificación de identidad, la comercialización masiva y la apertura de cuentas bancarias para facilitar el blanqueo de dinero. La usurpación de identidad y la actividad fraudulenta subsiguiente no forman parte necesariamente de un solo proceso delictivo, ya que los mercados delictivos en línea como los foros de tarjetas ofrecen a los ciberdelincuentes vías convenientes y eficientes para proporcionar los datos robados a personas que pueden utilizarlos para cometer fraudes[255].

ESTUDIO DE CASO: VIOLACIÓN DE DATOS

Un grupo delictivo organizado pirateó las redes de computadoras de múltiples empresas, lo que dio lugar a una violación de datos a gran escala y el consiguiente robo de los números de 160 millones de tarjetas de crédito. El grupo utilizó un programa malicioso para atacar los sistemas empresariales e infiltrarse en ellos. Para ocultar su actividad usó un programa malicioso que no podía ser detectado por los programas antivirus y arrendó servidores inaccesibles a las fuerzas del orden ("alojamientos web a prueba de balas"). Los números de tarjetas de crédito y la información personal conexa que fueron objeto de robo se vendieron por lotes. Los compradores codificaron los datos robados sobre las bandas magnéticas de tarjetas bancarias plásticas que utilizaron para retirar efectivo de las cuentas o realizar compras no autorizadas.

Fuente: *United States v. Drinkman, Kalinin, Kotov, Rytikov, Smilianets*, disponible en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).

Blanqueo de dinero

Un aspecto fundamental que consideran quienes cometen un fraude es la manera de enmascarar el origen ilegal de los fondos robados. Por blanqueo de dinero se entiende la adquisición, posesión, utilización, ocultación, conversión o transferencia de bienes, a sabiendas de que tales bienes son producto del delito[256].

Los grupos delictivos organizados dependen de varios procesos para acceder a los fondos robados sin que se activen los controles del sector financiero u otros sectores ni dejar ningún rastro financiero que pueda ser detectado por las fuerzas del orden[257]. Además de las transferencias electrónicas a través de las empresas bancarias y de tecnofinanzas, el producto del fraude, como cualquier otro delito que genera beneficios ilícitos, puede blanquearse usando mulas de dinero y empresas fantasma[258], comprando bienes inmuebles o bienes de gran valor, como autos, o utilizando oficinas de cambio de divisas, casinos, empresas pantalla o sistemas informales de transferencia de fondos, como las operaciones *hawala*[259].

La globalización del comercio y las finanzas, facilitada por el crecimiento, la diversificación y los adelantos tecnológicos en el sector financiero, ha creado nuevos canales en evolución que pueden ser aprovechados

[255] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (Luxemburgo, Oficina de Publicaciones de la Unión Europea).

[256] Convención contra la Delincuencia Organizada, art. 6. Véase también Benjámin Villányi, "Money laundering: history, regulations, and techniques", *Criminology and Criminal Justice*, 26 de abril de 2021.

[257] INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 18.

[258] Grupo de Acción Financiera, INTERPOL y Grupo Egmont de Unidades de Inteligencia Financiera, *Illicit Financial Flows from Cyber-Enabled Fraud* (París, 2023).

[259] Unidad de Inteligencia Financiera de Nigeria, "Nigeria releases money-laundering typologies through fraud report"; y UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia*.

por los delincuentes interesados en blanquear el producto del delito[260]. Constantemente, los delincuentes se adaptan a los nuevos canales en evolución que facilitan el movimiento rápido de fondos y capital a través de las fronteras nacionales y sacan provecho de ellos[261]. Un ejemplo al respecto son los delincuentes que utilizan como método el blanqueo de dinero a través del comercio, que consiste en "el proceso de ocultación del producto del delito y de traslado del valor a través de operaciones comerciales en un intento de conferir legitimidad al origen ilícito del producto". El blanqueo de dinero a través del comercio se concreta normalmente mediante la facturación fraudulenta de operaciones comerciales internacionales. Con la declaración fraudulenta del precio, la cantidad o la calidad de los bienes, los delincuentes pueden mover con rapidez cantidades de dinero o valores considerables de una jurisdicción a otra[262]. Los complejos mecanismos y operaciones comerciales transfronterizos dificultan considerablemente la capacidad de los órganos de aplicación de la ley y la industria para rastrear el origen de los bienes y distinguir la actividad financiera y comercial ilegítima de la legítima[263]. Tal vez resulte necesaria una cooperación internacional eficaz para rastrear los fondos robados que se blanquean de esa manera.

Las criptomonedas se utilizan cada vez más para blanquear el producto de delitos graves y actos de delincuencia organizada, y el fraude es uno de los delitos determinantes más comunes cuando se trata de dinero blanqueado por esa vía[264]. La compra de criptomonedas y su utilización para transferir fondos contribuye al anonimato y facilita la transferencia internacional de fondos de manera que disipa el rastro financiero y oculta el origen delictivo del dinero. Habitualmente supone la transferencia de criptodivisas y otros bienes digitales a través de diferentes redes de cadena de bloques (o monedas) para borrar el rastro, antes de cobrar el dinero convirtiéndolo de nuevo en dinero fíat[265]. Esto ayuda a evadir los rigurosos controles contra el blanqueo de dinero que aplican las instituciones financieras tradicionales. La imposición de una regulación sólida plantea dificultades, sobre todo debido al crecimiento de las finanzas descentralizadas[266]. Esos servicios facilitan la transferencia de criptodivisas a otros activos virtuales sin necesidad de un intermediario centralizado que podría detectar la actividad sospechosa y señalarla a la atención de las autoridades[267]. Los sitios de cambio de criptomonedas son numerosos y pueden utilizarse para transferir activos virtuales entre plataformas o convertir la criptodivisa en dinero fíat. Algunos de esos sitios carecen de licencia o están situados en países con poca reglamentación o que optan por aplicar pocos controles para prevenir el blanqueo de dinero (véase el estudio de caso que se presenta más adelante)[268].

La capacidad y los recursos para blanquear dinero son muy apreciados por los delincuentes vinculados al fraude organizado, y los procesos de blanqueo de dinero pueden representar un elemento de

---

[260] Emilia A. Isolauri e Irfan Ameer, "Money laundering as a transnational business phenomenon: a systematic review and future agenda", *Critical Perspectives on International Business*, vol. 19, núm. 3 (abril de 2023); Europol, *The Other Side of the Coin: An Analysis of Financial and Economic Crime*, European Financial and Economic Crime Threat Assessment 2023 (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2023); y Pierre Bardin *et al.*, "Money laundering poses a risk to financial sector stability", Blog del Fondo Monetario Internacional, 4 de septiembre de 2023.

[261] Isolauri y Ameer, "Money laundering as a transnational business phenomenon".

[262] Grupo de Acción Financiera, "Trade based money laundering" (París, 2006).

[263] Véase, por ejemplo, James Treadwell, "From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace", *Criminology and Criminal Justice*, vol. 12, núm. 2 (abril de 2012).

[264] Este es el *modus operandi* que utilizan con más frecuencia quienes cometen fraudes en Europa (INTERPOL, "Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas", pág. 17; y Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, Europol Spotlight Report Series (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2021).

[265] Vladlena Benson, Umut Turksen y Bogdan Adamyk, "Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities", *Journal of Financial Regulation and Compliance*, vol. 32, núm. 1 (enero de 2024).

[266] Las finanzas descentralizadas consisten en un sistema de productos y servicios financieros que emplea contratos inteligentes sobre cadenas de bloques para la gestión de operaciones financieras entre dos partes. Esa tecnología permite que se produzcan intercambios automatizados en que las personas pueden comerciar directamente entre sí, con lo que elimina la necesidad de que intervenga una institución centralizada o un tercero (p. ej., un banco o un proveedor de servicios de criptomonedas). Véase, por ejemplo, Organización de Cooperación y Desarrollo Económicos, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (2022).

[267] Benson, Turksen y Adamyk, "Dark side of decentralised finance".

[268] Véase, por ejemplo, Fiscalía de los Estados Unidos, Distrito Sur de Nueva York, "Tornado cash founders charged with money laundering and sanctions violations", comunicado de prensa, 23 de agosto de 2023.

organización decisivo que impulsa la formación de un grupo delictivo organizado[269]. Los facilitadores profesionales desempeñan un papel clave en algunas tramas fraudulentas, particularmente las que se aprovechan de estructuras comerciales legales para blanquear el producto del delito[270]. En varios estudios se ha puesto de relieve el papel prominente que desempeñan abogados, contables, asesores financieros, gestores bancarios y corredores hipotecarios como facilitadores del blanqueo del producto del delito[271]. Esto se refiere al uso que hacen los autores de fraudes de las redes de blanqueo de dinero profesionales[272], profesionales que son sobornados y otros que inconscientemente facilitan el blanqueo de dinero, a veces por no observar los procedimientos de diligencia debida. Es importante llevar a cabo investigaciones específicas sobre blanqueo de dinero respecto de los profesionales que cobran comisión por prestar servicios a múltiples grupos delictivos organizados.

Algunos grupos delictivos organizados reclutan a delincuentes con capacidad especializada en el blanqueo de dinero, como los que anuncian sus servicios en mercados delictivos en línea. Esto puede resultar especialmente útil para facilitar el fraude transnacional, en el que los coautores en el país objetivo (es decir, donde se encuentran las víctimas) reciben y transfieren los fondos robados hacia el extranjero[273]. La captación de mulas de dinero consiste en pagar una comisión a una persona para que reciba fondos ilícitos en sus propias cuentas bancarias y después los transfiera a una cuenta controlada por el delincuente. Esto sirve para dispersar los fondos robados y así reducir el riesgo de detección por parte de los proveedores de servicios financieros. Los autores de fraudes emplean diversos métodos para reclutar a las mulas de dinero, como la colocación de anuncios en línea y la captación en la comunidad local[274]. Pueden captarlas en redes sociales existentes o en grupos de personas con necesidades financieras (p. ej., niños y jóvenes o estudiantes universitarios) o en contextos de vulnerabilidad, y pueden convertirlas también en víctimas de fraude[275].

ESTUDIO DE CASO: FACILITACIÓN DEL BLANQUEO DE DINERO

Se sospecha que un cambio de moneda virtual registrado en Costa Rica facilitó el blanqueo de 6.000 millones de dólares. Previo pago de una pequeña comisión, los usuarios podían depositar dinero fíat y convertirlo en moneda digital, y después transferir ese dinero a otros usuarios. La empresa registraba datos mínimos sobre los usuarios del servicio y las autoridades pensaron que la empresa había sido concebida con la intención de ocultar la identidad de sus usuarios y de que fuera imposible rastrearlos. El servicio era utilizado por ciberdelincuentes vinculados a diversos delitos determinantes, como el fraude con tarjetas de crédito y la usurpación de identidad.

Fuente: Yongyu Zeng y David Buil-Gil, "Organizational and organized cybercrime", en *Oxford Research Encyclopedia of Criminology and Criminal Justice*, H. Pontell, ed. (Oxford, Oxford University Press, 2023).

[269] Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

[270] Europol, *The Other Side of the Coin*.

[271] Michael Levi, "Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation", *Trends in Organized Crime*, vol. 24, núm. 1 (marzo de 2021); y May y Bhardwa, *Organised Criminal Groups Involved in Fraud*.

[272] Grupo de Acción Financiera, INTERPOL y Grupo Egmont de Unidades de Inteligencia Financiera, *Illicit Financial Flows from Cyber-Enabled Fraud*, pág. 15.

[273] Manny Aston *et al.*, "A preliminary profiling of internet money mules: an Australian perspective", en *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (2009); Conradt, "Online auction fraud and criminological theories"; y Whittaker y Button, "Understanding pet scams".

[274] Leukfeldt y Jansen, "Cyber criminal networks and money mules"; y Soudijn y Zegers, "Cybercrime and virtual offender convergence settings".

[275] Skidmore y Aitkenhead, "Understanding the characteristics of serious fraud offending".

ESTUDIO DE CASO: FRAUDE ROMÁNTICO

En Nigeria se descubrió que dos hermanos habían cometido un fraude romántico probablemente dirigido contra un gran número de víctimas. Uno de los hermanos facilitaba el acceso a múltiples cuentas bancarias extranjeras, varias de las cuales aparecían a nombre de empresas que resultaron ser empresas pantalla. Las empresas y cuentas se crearon en colaboración con el gerente de un banco local y un coautor que se encontraba en China. Se depositaron considerables sumas de dinero en esas cuentas empresariales y, según los registros, una de las empresas tenía una facturación en dólares multimillonaria. Los autores del fraude en Nigeria vendían criptodivisas al coautor en China, y este era quien después realizaba los pagos en las cuentas empresariales.

Fuente: Unidad de Inteligencia Financiera de Nigeria, "Nigeria releases money-laundering typologies through fraud report", 12 de agosto de 2023.

Tecnología instrumental

La tecnología como medio para ocultar la delincuencia

La mayor disponibilidad de herramientas de cifrado desempeña un importante papel en la facilitación de ciberdelitos como el fraude, especialmente el empleo de redes privadas virtuales, el cifrado de extremo a extremo para las comunicaciones, la web oscura y los servicios de hospedaje a prueba de balas[276]. Muchas de esas tecnologías son legales y su disponibilidad es legítima (p. ej., los servicios de redes privadas virtuales), aunque los delincuentes diseñan y suministran algunas de ellas[277]. Si bien algunas de esas herramientas pueden tener usos legítimos para la población en general, también pueden servir para ocultar la identidad y facilitar comunicaciones e intercambios en línea seguros entre delincuentes. La web oscura es una capa cifrada de Internet en la que los usuarios pueden mantenerse ocultos e ilocalizables. Las criptomonedas constituyen un método de pago preferido en el intercambio de bienes y servicios ilícitos en la web oscura, lo que agrega otra capa de velo para dificultar aún más su rastreo[278]. A manera de ilustración cabe citar el caso de un mercado delictivo de grandes proporciones con un servicio oculto en la red Tor[279] que escondía la identidad de los usuarios y la ubicación de los servidores[280]. En un momento dado, el sitio tuvo 200.000 usuarios y se calcula que desde su creación las operaciones en el mercado alcanzaron un valor total de 1.000 millones de dólares; por lo general, las operaciones se realizaban en bitcoines u otras criptomonedas. En el sitio se ofrecía una serie de herramientas y recursos de carácter delictivo, como documentos de identidad falsos y dispositivos de acceso, mercancías falsificadas y otros servicios fraudulentos.

[276] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*; Europol, Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y Centro Europeo contra la Ciberdelincuencia, "First report of the observatory function on encryption" (La Haya, 2019); Europol y Eurojust Public Information, "Common challenges in combating cybercrime" (2019); y Annamaria Szakonyi, Brian Leonard y Maurice Dawson, "Dark web: a breeding ground for ID theft and financial crimes", en *Handbook of Research on Theory and Practice of Financial Crimes*, Abdul Rafay, ed. (Hershey (Pensilvania, Estados Unidos), IGI Global, 2021).

[277] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*.

[278] Szakonyi, Leonard y Dawson, "Dark web: a breeding ground for ID theft and financial crimes".

[279] Tor es un navegador que se utiliza para acceder a la web oscura.

[280] Europol, "Massive blow to criminal dark web activities after globally coordinated operation", 20 de julio de 2017.

La tecnología como medio para facilitar el engaño

La tecnología moderna ha industrializado metodologías de fraude que existían desde hace mucho tiempo[281]. Los entornos digitales aumentan la capacidad para comunicarse con las víctimas, realizar operaciones comerciales y financieras fraudulentas y aprovechar grandes conjuntos de datos. Además, las nuevas tecnologías creadas por agentes legítimos e ilegítimos han automatizado procesos que antes era laboriosos y costosos. Ejemplo de ello son el uso de bots para hacer miles de clics en un sitio web con el objetivo de manipular las puntuaciones de los motores de búsqueda (es decir, el fraude del clic) y los dispositivos de granjas SIM baratos y de fácil adquisición con múltiples tarjetas SIM para realizar llamadas fraudulentas o enviar grandes volúmenes de mensajes de texto a posibles víctimas.

Un factor decisivo de la evolución de las metodologías de fraude es la necesidad que tienen los delincuentes de adaptarse constantemente a las medidas de seguridad compensatorias adoptadas por el Estado o la industria[282]. Ejemplo de ello es el aumento del fraude sin presencia de tarjeta, que surgió en respuesta a la introducción de las tarjetas con chip y PIN para aumentar su seguridad[283]. Entre otros ejemplos más recientes cabe citar el surgimiento del robo de huella digital de los dispositivos con el propósito de contrarrestar el mayor uso de datos biométricos para la autenticación de la identidad y el acceso a las cuentas[284]. Las tecnologías de inteligencia artificial encierran el potencial de aumentar ese entorno contencioso pues incrementan la capacidad de los delincuentes para cometer fraudes y al mismo tiempo también ofrecen a las organizaciones la posibilidad de mejorar sus medios de ciberdefensa[285].

Es probable que los adelantos operados en el ámbito de la inteligencia artificial, en particular la inteligencia artificial generativa, capaz de generar contenido que imita características humanas, desempeñen un papel decisivo en las formas que adoptará el fraude en el futuro. Se prevé que la capacidad de los autores de fraudes se incremente de dos maneras, a saber: a) con el aumento del alcance y el volumen de los actos delictivos al facilitar la producción de mayores cantidades de contenido fraudulento con mayor rapidez, y b) con el perfeccionamiento de los métodos de ingeniería social existentes al producir contenido más sofisticado, convincente y personalizado[286].

Se ha constatado la utilización de la inteligencia artificial en los siguientes aspectos del fraude:

- Preparación y focalización sobre el objetivo. Las tecnologías de inteligencia artificial aumentan la capacidad de los delincuentes para procesar y analizar grandes volúmenes de datos a fin de detectar vulnerabilidades e inmediatamente procesar datos robados para extraer más información de valor[287]. Con la inteligencia artificial generativa será posible diseñar y producir un contenido más refinado y específico con velocidad, como textos, imágenes y documentos que facilitarían el fraude[288]. FraudGPT, una herramienta de inteligencia artificial generativa concebida para facilitar la ciberdelincuencia, es capaz de automatizar una serie de tareas, entre otras, la creación de materiales fraudulentos como mensajes de correo electrónico[289].

---

[281] Button y Cross, *Cyber Frauds, Scams and Their Victims*.

[282] Albanese, "Fraud".

[283] Michael Levi, "Organising and controlling payment card fraud: fraudsters and their operational environment", *Security Journal*, vol. 16, núm. 2 (abril de 2003).

[284] Europol, "Online fraud schemes".

[285] Borja Álvarez Martínez *et al.*, "Mapping the state of the art: artificial intelligence for decision-making in financial crime", en *Cybersecurity for Decision Makers*, Narashima Rao Yajihala y Kenneth David Strang, eds. (Boca Ratón (Florida, Estados Unidos, CRC Press, 2023). https://www.routledge.com/Cybersecurity-for-Decision-Makers/Vajjhala-Strang/p/book/9781032334974?srsltid=AfmBOoqL0-ovS3IO4TG_gXX5etTA9rOcLN0rjwAxlbsccdVeH4w-ICPo.

[286] PricewaterhouseCoopers y Stop Scams UK, "Impact of artificial intelligence on fraud and scams" (2023), pág. 9.

[287] Reino Unido, Centro Nacional de Ciberseguridad, "The near-term impact of AI on the cyber threat" (2024).

[288] PricewaterhouseCoopers y Stop Scams UK, "Impact of artificial intelligence on fraud and scams".

[289] Falade, "Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 9, núm. 5 (septiembre/octubre de 2023).

- Ingeniería social. Las tecnologías de clonación de voz y de ultrafalsificación o *deepfake* aumentan la capacidad de los delincuentes para hacerse pasar por otras personas o entidades que gozan de la confianza de las víctimas para promover productos o servicios fraudulentos.
- Evasión de la detección. El mayor uso de la tecnología de inteligencia artificial en la comisión de fraudes puede llegar a aumentar el anonimato y esfumar aún más cualquier rastro que pueda llevar hasta los delincuentes responsables[290].

Se ha señalado que los autores de fraudes son ávidos usuarios de la ciberdelincuencia como servicio y que utilizan las herramientas y datos que se ofrezcan[291]. Se prevé que la mayor disponibilidad legítima de la tecnología de inteligencia artificial y el incremento de la oferta de ciberherramientas facilitadas por la inteligencia artificial en los mercados delictivos sumergidos servirán para aumentar la capacidad de potenciales autores de fraudes que posean menos conocimientos técnicos[292]. Como consecuencia, disminuirán los obstáculos para involucrarse en el fraude organizado.

En la presente sección se han puesto de relieve algunas de las técnicas y recursos que desempeñan un papel subyacente decisivo en la facilitación de las múltiples variantes del fraude organizado. También se ha destacado la amplia variedad de vías utilizadas por los autores de fraudes para comunicarse con las víctimas y engañarlas, así como las diversas técnicas empleadas para frustrar los esfuerzos de los organismos encargados de hacer cumplir la ley y evitar el riesgo de ser descubiertos y castigados. Esos métodos están en constante evolución, a menudo al ritmo de cambios mundiales legítimos en las comunicaciones, las finanzas, el comercio y la tecnología. Es importante que los Estados Miembros, en alianza con industrias clave como los sectores financiero y tecnológico, descubran y controlen los métodos subyacentes que utilizan los autores de fraudes a fin de adoptar medidas de respuesta estratégica eficaces para prevenir esos delitos.

[290] Véase www.acfeinsights.com/acfe-insights/2023/1/6/ai-and-fraud.
[291] Europol, "Online fraud schemes".
[292] Reino Unido, Centro Nacional de Ciberseguridad, "The near-term impact of AI on the cyber threat".

CAPÍTULO V

Combatir el fraude organizado

El fraude organizado se perpetra en grandes volúmenes y penetra en muchos sectores comerciales y financieros. Para los autores, las recompensas son grandes y los obstáculos y los riesgos son bajos. Una respuesta integral incluye estrategias de prevención de la delincuencia y leyes adecuadas para cerrar el paso a las abundantes oportunidades para perpetrar estos delitos, junto con una firme labor de aplicación de la ley para perseguir y disuadir a los delincuentes. Se necesitan controles más eficaces para hacer frente a las vulnerabilidades técnicas de las infraestructuras y los sistemas, así como para educar y sensibilizar a los sectores público y empresarial a fin de contribuir a la defensa contra el fraude. Las respuestas estratégicas deberían tener en cuenta los siguientes principios[293]:

- Prevenir la (re)infiltración de la delincuencia organizada en las comunidades, la economía y las instituciones políticas
- Perseguir a los grupos delictivos organizados y sus ganancias ilícitas, aumentando de ese modo sus costos y riesgos operacionales
- Proteger a las personas vulnerables y a las víctimas para que no sufran (más) daños
- Promover las asociaciones y la cooperación a todos los niveles, también a través de las fronteras internacionales, con un enfoque que abarque a toda la sociedad

Las estrategias contra la delincuencia organizada deben tener en cuenta las complejidades del problema del fraude organizado, especialmente porque es transnacional, explota tecnologías y sistemas mundiales y se adapta continuamente a los cambios de los sistemas comerciales y financieros. El cambio depende de políticas que adopten un enfoque múltiple que coordine las respuestas de distintos departamentos y organismos gubernamentales, los sectores clave de la industria privada y la sociedad civil. También se necesita una mayor colaboración internacional para comprender y afrontar el fraude organizado transfronterizo.

Estas estrategias integrales contra la delincuencia organizada que implican a toda la sociedad son especialmente importantes en contextos en que los grupos delictivos organizados están implicados cada vez más en diversas formas de delincuencia organizada[294], incluido el fraude organizado. Las estrategias aisladas o las respuestas centradas en un solo ámbito, como garantizar los resultados de la justicia penal, no alcanzarían para combatir el carácter multidimensional de los grupos delictivos organizados implicados en la comisión de múltiples delitos. Además, la falta de coordinación en las respuestas a los

[293] UNODC, *Guía práctica para elaborar estrategias de alto impacto contra la delincuencia organizada* (Viena, 2021).

[294] Véanse, por ejemplo, UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*; y Subdivisión de Investigación y Análisis de Tendencias de la UNODC y Oficina Regional para África Occidental y Central de la UNODC, "Impact of transnational organized crime on stability and development in the Sahel" (Viena, 2024). https://www.unodc.org/documents/data-and-analysis/tocta_sahel/TOCTA_Sahel_Transversal_2024.pdf.

distintos tipos de delitos puede crear lagunas, duplicar esfuerzos y utilizar inadecuadamente los limitados recursos. Las estrategias regionales y nacionales contra la delincuencia organizada estructuradas en torno a los cuatro pilares antes mencionados (prevenir, perseguir, proteger y promover) pueden servir de marco general que se complemente con respuestas adaptadas a cada delito, como planes de acción, centros de coordinación y grupos de trabajo contra el fraude organizado.

LISTA DE VERIFICACIÓN PARA EL EXAMEN DE ESTRATEGIAS Y LA ELABORACIÓN DE PLANES DE ACCIÓN CONTRA EL FRAUDE

PREVENIR el fraude organizado

- ☐ Análisis estratégico para identificar y evaluar las causas económicas, culturales, sociales e institucionales de la marginación y la vulnerabilidad que crean las vías para la participación en el fraude
- ☐ Respuestas para desviar o disuadir a los grupos vulnerables de ser reclutados o arrastrados de otro modo al fraude. Esto incluye dirigirse a quienes, en sectores y profesiones clave, son vulnerables a la corrupción, y tomar medidas para fomentar la denuncia y proteger a víctimas, testigos, informantes y denunciantes
- ☐ Medidas para cuestionar las narrativas de los grupos delictivos organizados que reclutan a personas para cometer fraude

PERSEGUIR a los grupos delictivos organizados

- ☐ Legislación en vigor para la penalización del fraude, incluida, cuando proceda, la tipificación del fraude como delito grave, de conformidad con el artículo 2 b) de la Convención contra la Delincuencia Organizada. Las sanciones deben ser disuasorias, proporcionadas y claras y estar aseguradas, y deben evitar toda violación de los derechos humanos o constitucionales
- ☐ Organismos encargados de hacer cumplir la ley y un poder judicial dotados de los conocimientos técnicos para investigar eficazmente el fraude organizado, incluida la investigación financiera, la investigación de la ciberdelincuencia, la ciencia forense digital y las técnicas especiales de investigación pertinentes, y para identificar, localizar, embargar preventivamente y decomisar el producto del delito y otros activos e incautarse de ellos
- ☐ Sistemas de bases de datos para compilar y analizar los datos de las entidades nacionales encargadas de hacer cumplir la ley a fin de facilitar la identificación de los grupos delictivos organizados y fundamentar las respuestas estratégicas y tácticas al fraude organizado

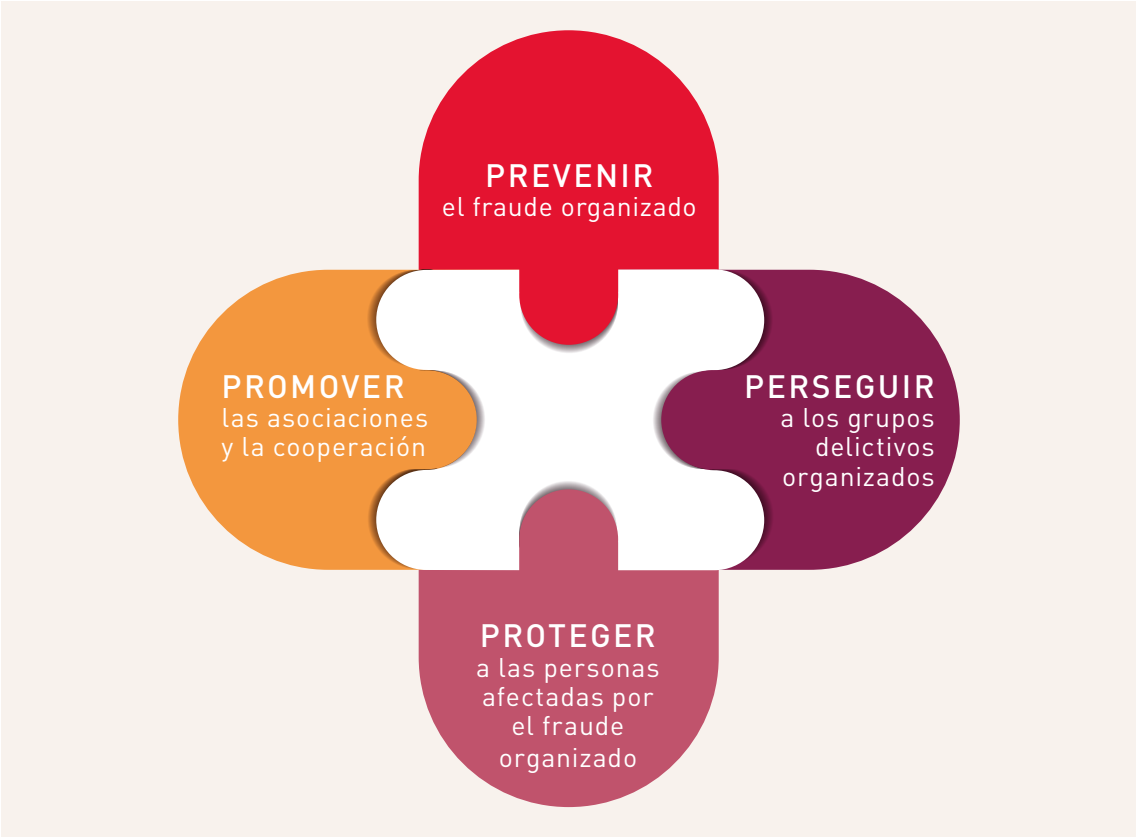
PROTEGER a las personas afectadas por el fraude organizado

- ☐ Campañas de sensibilización de la ciudadanía y la comunidad empresarial para fomentar comportamientos seguros y la protección a fin de evitar ser víctimas de fraude
- ☐ Medidas para identificar y apoyar a las víctimas en situación vulnerable y en riesgo de sufrir fraudes reiterados y daños graves

PROMOVER las asociaciones y la cooperación

- ☐ Estrategia de prevención y lucha contra el fraude que abarque a toda la sociedad, incluidos el sector privado, la sociedad civil, el mundo académico y los agentes educativos, según proceda
- ☐ Cauces de denuncia claros para que el público y la comunidad empresarial puedan denunciar el fraude a las entidades encargadas de hacer cumplir la ley y acceder al apoyo necesario
- ☐ Medidas legislativas y de otro tipo para orientar el intercambio de información entre el Estado y el sector privado, incluidas las empresas de sectores clave como las finanzas y la tecnología
- ☐ Medidas para impulsar el compromiso estratégico con los organismos empresariales e industriales de sectores privados clave, detectar las debilidades y vulnerabilidades sistémicas y coordinar respuestas estratégicas eficaces para prevenir el fraude
- ☐ Marcos para fomentar la cooperación internacional en asuntos penales, entre otras cosas mediante la asistencia judicial recíproca y los equipos conjuntos de investigación

FIGURA. CUATRO PILARES ESTRATÉGICOS PARA COMBATIR EL FRAUDE ORGANIZADO



Prevenir el fraude organizado

Pueden llevarse a cabo campañas de prevención e intervenciones específicamente dirigidas a disuadir a las personas de la comisión de delitos de fraude organizado. Las investigaciones al respecto son escasas, pero en algunas subculturas, los autores de fraudes y ciberdelitos gozan de legitimidad social. Las personas pertenecientes a estas comunidades y redes pueden adoptar diversas narrativas para justificar su conducta delictiva; algunos ejemplos son la opinión de que las víctimas reciben lo que se merecen (p. ej., que son avariciosas) o actitudes que minimizan los delitos y daños causados por el fraude[295]. Además, el fraude puede ofrecer a los delincuentes un medio de lograr un éxito en el plano material que de otro modo sería inalcanzable, sobre todo en regiones donde la pobreza es elevada y escasean las perspectivas legítimas. En algunos casos, los autores de fraudes pasan a ser personas destacadas en el ámbito local y hacen ostentación pública de riqueza, lo que los convierte en figuras que los jóvenes aspiran a imitar. Algunos jóvenes se dedican a la ciberdelincuencia sin ser conscientes de que están cometiendo un delito o causando daños[296]. Estos delitos pueden constituir un fraude de bajo nivel, pero conllevan el riesgo de que los delincuentes se vean atraídos por la perspectiva de obtener beneficios del delito y pasen al fraude organizado. Es necesario comprender las modalidades y las vías del fraude organizado dentro de los contextos sociales, económicos y políticos locales, y orientar las intervenciones para abordar las causas profundas de los delitos de fraude[297].

[295] Véanse, por ejemplo, Shover, Coffey y Sanders, "Dialing for dollars"; y Whitty, "419: it's just a game".

[296] Mary Aiken, Julia Davidson y Philipp Amann, "Youth pathways into cybercrime" (2016).

[297] Véase, por ejemplo, Lorenzo Pasculli, "Coronavirus and fraud in the UK: from the responsibilisation of the civil society to the deresponsibilisation of the state", *Coventry Law Journal*, vol. 25, núm. 2 (diciembre de 2020).

Los grupos delictivos organizados implicados en fraudes incorporan asociaciones poco sólidas con personas que son esenciales para facilitar el delito pero que adoptan un papel periférico en el engaño. Esto incluye a personas que desempeñan tareas profesionales que facilitan el fraude (p. ej., profesionales del derecho y las finanzas) y miembros del público que proporcionan el uso de sus cuentas a cambio de una comisión (es decir, mulas de dinero). Para estos coautores, los niveles de complicidad y culpabilidad pueden ser ambiguos, y algunos se contentan con aceptar el dinero sin hacer demasiadas preguntas sobre los delitos subyacentes. Las campañas de información pública dirigidas a estos grupos de riesgo con el fin de poner de relieve la gravedad del delito y el riesgo de ser objeto de sanciones de la justicia penal pueden servir para aumentar la conciencia de estos delitos y desviar y disuadir a las personas de participar en ellos.

ESTUDIO DE CASO: DESVIAR A LOS JÓVENES DE LA CIBERDELINCUENCIA

En respuesta al aumento del volumen de jóvenes que entran en contacto con el sistema de justicia penal por delitos de piratería informática, el Reino de los Países Bajos creó el programa de rehabilitación Hack_Right para delincuentes primerizos de entre 12 y 30 años de edad. El programa sirve para generar conciencia sobre la ley, las consecuencias de la piratería informática y el impacto en las víctimas. El objetivo del programa es apartar a la gente de la ciberdelincuencia y otros delitos potencialmente más graves (como el fraude organizado) y reorientar esas habilidades hacia actividades legítimas.

Fuente: J. A. M. Schiks, Susanne van 't Hoff-de Goede y E. Rutger Leukfeldt, "An alternative intervention for juvenile hackers? A qualitative evaluation of the Hack_Right intervention", *Journal of Crime and Justice* (2023).

Perseguir a los grupos delictivos organizados

Legislación

La adopción de marcos jurídicos claros y sólidos es importante para evaluar y enfrentar el fraude, a fin de que los profesionales puedan identificar con seguridad la presencia de delincuencia organizada y asignar los recursos e intervenciones correspondientes. Además, la cooperación internacional depende de que en las distintas jurisdicciones legales exista un entendimiento claro y común de lo que constituye fraude organizado, guiado por las disposiciones de la Convención contra la Delincuencia Organizada.

Algunos Estados Miembros han promulgado legislación especializada para afrontar los delitos relacionados con el fraude, mientras que otros han incorporado estos delitos a sus códigos penales. El fraude también puede abordarse en múltiples leyes, con lo que se generan varias definiciones. Se necesitan marcos jurídicos que ofrezcan en medida suficiente:

- Claridad, para facilitar la comprensión de los profesionales y garantizar la aplicación efectiva de la ley y una delimitación clara de los comportamientos lícitos e ilícitos
- Cobertura, que debe ser lo suficientemente amplia y flexible como para captar la diversidad de métodos utilizados para cometer fraude, incluidos los métodos emergentes y futuros, como los que explotan las nuevas tecnologías[298]

Algunos países han adoptado definiciones legales de fraude muy específicas y preceptivas que enumeran los diversos productos, servicios o técnicas que constituyen una actividad fraudulenta en el marco de la ley, entre las que se cuentan el uso de la información personal de una víctima, la suplantación de

[298] Véase, por ejemplo, Ben Summers, "The Fraud Act 2006: has it had any impact?", *Amicus Curiae*, núm. 75 (2008).

una autoridad o la creación de una falsa esperanza de ganar algo. Otros emplean definiciones jurídicas amplias que pueden aplicarse a una serie de situaciones o contextos delictivos (véase el cap. I). El fraude es muy diverso en cuanto a los métodos empleados por los autores y el impacto en las víctimas o los efectos más amplios. Así, los marcos de imposición de penas de los países varían, incluida la presencia de factores agravantes y atenuantes, que pueden referirse a la experiencia de la víctima, las características de los autores de estos delitos y la comisión de determinadas categorías de fraude[299].

La combinación de factores agravantes incluidos en la legislación puede determinar los tipos de delitos de fraude y la pena máxima, que puede variar según los Estados. En algunos marcos jurídicos se ha adoptado una perspectiva centrada en la víctima, mientras que otros se centran en las características de los delincuentes y sus métodos. Para determinar el impacto del delito, algunos países se fijan en las pérdidas económicas como proporción de los ingresos anuales de la víctima, o en la suma de dinero robado, si se han utilizado dispositivos informáticos o si está implicado un reincidente o un grupo delictivo organizado (véanse los ejemplos que se presentan a continuación).

EJEMPLO DE LEGISLACIÓN: MÉXICO

CÓDIGO PENAL FEDERAL

Artículo 386. Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El delito de fraude se castigará con las penas siguientes:

a) con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de 10 veces el salario;

b) con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario;

c) con prisión de 3 a 12 años y multa hasta de 120 veces el salario, si el valor de lo defraudado fuere mayor de 500 veces el salario.

[299] Estos factores se recopilan para resumir los marcos jurídicos de los distintos países. No todos los factores estaban presentes en los marcos legislativos de cada país. Entre los ejemplos de factores agravantes pueden contarse los siguientes: experiencia de la víctima (gran impacto financiero u otro impacto personal (p. ej., infundir miedo o sensación de peligro en la víctima)); grandes pérdidas económicas a las personas o a diversas víctimas; gran escala en términos de volumen de víctimas y/o cantidad de dinero perdido; atacar a víctimas que son vulnerables de algún modo; atacar al Estado, instituciones públicas u organizaciones benéficas; características de quien comete fraude (participación de un grupo o banda delictiva organizada; delincuentes reincidentes); y categorías de fraude (fraude informático o electrónico; que impliquen la emisión de acciones, bonos, *warrants* o títulos; que impliquen suplantación de un funcionario público, abuso de un cargo oficial o abuso de relaciones personales).

EJEMPLO DE LEGISLACIÓN: UZBEKISTÁN

CÓDIGO PENAL

Artículo 168. Fraude

El fraude, es decir, la adquisición de bienes pertenecientes a alguien o del derecho a esos bienes mediante engaño o abuso de confianza,

será castigado con multa de hasta 100 salarios mínimos mensuales, o trabajos correccionales de hasta 1 año o prisión de hasta 6 meses.

El fraude cometido:

a) a gran escala;

b) repetidamente o por un reincidente peligroso;

c) por concierto previo de un grupo de personas;

d) con ayuda de dispositivos informáticos;

será castigado con multa de entre 100 y 300 salarios mínimos mensuales, o trabajos correccionales de hasta 2 años o prisión de hasta 5 años.

El fraude cometido:

a) a gran escala;

b) por un reincidente especialmente peligroso;

c) por un grupo organizado o en su interés;

será castigado con multa de entre 300 y 600 salarios mínimos mensuales, o trabajos correccionales de hasta 3 años o prisión de entre 5 y 10 años.

En caso de reparación del daño patrimonial, no se aplicará la pena de prisión.

Las bandas de penas también son muy diversas. En algunos países (p. ej., el Uruguay), la pena máxima es de 4 años de prisión, mientras que en otros (p. ej., los Estados Unidos) se prevén penas de hasta 30 años de prisión. En algunos otros países, no existen bandas de penas estipuladas, y las condenas dependen probablemente de la discrecionalidad del fiscal o de la aplicación de un criterio general para determinar la gravedad del delito.

EJEMPLO DE LEGISLACIÓN: ESTADOS UNIDOS DE AMÉRICA

TÍTULO 18

Artículo 1344. Fraude bancario

Se impondrá a quien ejecute o intente ejecutar a sabiendas un plan o artificio con el fin de:

a) defraudar a una institución financiera; o

b) obtener cualquiera de los dineros, fondos, créditos, activos, valores u otros bienes propiedad de una institución financiera, o bajo su custodia o control, mediante pretensiones, representaciones o promesas falsas o fraudulentas,

una multa no superior a 1.000.000 de dólares o una pena de prisión no superior a 30 años, o ambas.

Aplicación de la ley

Las entidades encargadas de hacer cumplir la ley desempeñan un papel importante en el marco de una estrategia más amplia centrada en la prevención del fraude y la protección de los ciudadanos. La justicia penal puede actuar para disuadir a los delincuentes o posibles delincuentes, prevé el castigo, protege a la sociedad de los delincuentes perjudiciales y refuerza los valores sociales sobre los comportamientos aceptados[300]. La capacidad de hacer cumplir la ley con firmeza se ve afectada por los factores que se exponen a continuación.

Evaluar y combatir el fraude organizado

En el contexto de las demandas variadas y contrapuestas que plantea la delincuencia organizada, los recursos policiales suelen gravitar hacia delitos distintos del fraude[301]. En la lucha contra el fraude organizado, es posible que las sentencias penales sean insuficientes, que falte información y, lo que es quizá más importante, que no haya certezas sobre la forma de integrar el fraude en las políticas dirigidas a combatir la delincuencia grave y organizada. La incapacidad para identificar estas intersecciones puede hacer que las medidas dirigidas a hacer cumplir la ley no abarquen a quienes cometen actos de fraude. Unos marcos políticos y legislativos claros y sólidos ayudan a definir con mayor claridad los casos de fraude que constituyen actos de delincuencia grave y organizada y refuerzan las evaluaciones de las entidades encargadas de hacer cumplir la ley para orientar los recursos para una investigación penal proactiva.

Investigación penal

En muchas regiones se teme que la policía no esté preparada o equipada para hacer frente al crecimiento del ciberfraude. Esto se debe en parte a las políticas, los sistemas y la cultura en lo relativo al cumplimiento de la ley, que han tenido dificultades para adaptarse a este nuevo panorama delictivo[302]. Algunos organismos encargados de hacer cumplir la ley han creado unidades especializadas en la investigación del fraude y la ciberdelincuencia, normalmente centradas en llevar a cabo las investigaciones más complejas para perseguir a los delincuentes de mayor riesgo[303]. Los recursos clave incluyen la capacidad de llevar a cabo una investigación digital eficaz, profesionales con experiencia en investigación financiera y ciencia forense digital, y tecnología para facilitar los procedimientos de investigación.

Disrupción

El fraude organizado puede perpetrarse en grandes volúmenes y a una velocidad que a menudo choca con la lentitud de las investigaciones de fraude complejas. La disrupción puede basarse en una amplia gama de técnicas y capacidades de que disponen las entidades encargadas de hacer cumplir la ley y las organizaciones asociadas a ellas para ofrecer tácticas más diversas que impidan a los delincuentes delinquir y reduzcan así el riesgo de nuevos daños a la población[304]. Las tácticas pueden dirigirse contra los actos, los agentes o los entornos criminógenos, con ejemplos clave como la retirada de sitios web; la

[300] Button *et al.*, *Fraud and Punishment*.

[301] Doig y Levi, "A case of arrested development?".

[302] Adam M. Bossler y Tom J. Holt, "Patrol officers' perceived role in responding to cybercrime", *Policing: An International Journal of Police Strategies and Management*, vol. 35, núm. 1 (marzo de 2012); y Barry Loveday, "Still plodding along? The police response to the changing profile of crime in England and Wales", *International Journal of Police Science and Management*, vol. 19, núm. 2 (abril de 2017).

[303] Mark Button y Martin J. Tunley, "Explaining fraud deviancy attenuation in the United Kingdom", *Crime Law and Social Change*, vol. 63, núms. 1 y 2 (marzo de 2015); y Dale Willits y Jeffrey Nowacki, "The use of specialized cybercrime policing units: an organizational analysis", *Criminal Justice Studies*, vol. 29, núm. 2 (abril de 2016).

[304] Michael Skidmore, "Lifting the lid on 'disruption' as an approach to controlling serious and organised crime", *Perspectives on Policing Paper*, núm. 9 (Londres, The Police Foundation, 2023).

incautación del producto de los delitos; la selección de personas clave de una red, como las que facilitan el blanqueo de dinero o suministran información personal robada, e intervenciones para desbaratar la codelincuencia, como tácticas para socavar la confianza en los mercados delictivos[305].

Cooperación internacional

Es habitual que los delincuentes, las víctimas, las tecnologías y otros facilitadores del fraude organizado sean transnacionales, lo que puede causar confusión respecto de la jurisdicción aplicable y obstaculizar las investigaciones penales localizadas. Esto se debe, entre otras cosas, a las dificultades para aprovechar rápidamente la asistencia judicial recíproca de otros países, en particular para adquirir y compartir datos y pruebas del sector privado con el fin de facilitar la investigación y el enjuiciamiento, así como los complejos procesos de extradición[306]. La cooperación internacional también es importante para incautarse del producto de los delitos y decomisarlo, devolver los bienes robados y garantizar la indemnización de las víctimas[307].

Plantilla diversificada

Las personas tienen diferentes experiencias con el sistema de justicia penal, debido a factores como el racismo, el sexismo, el capacitismo, la homofobia y la discriminación por motivos de estatus socioeconómico. La posibilidad de que estas experiencias se aborden adecuadamente es limitada debido a la continua infrarrepresentación de las mujeres y las personas de diversos orígenes en las entidades encargadas de hacer cumplir la ley, el sistema de justicia penal y los puestos con poder de decisión, si bien diversas investigaciones[308] han revelado que las mujeres agentes están mejor posicionadas para satisfacer las necesidades de las mujeres y las niñas en sus comunidades. A pesar de ello, la UNODC ha constatado que el porcentaje de mujeres policías en todos los países estudiados era de entre el 3 % y el 37 %[309].

[305] A modo de ejemplo, las fuerzas del orden de varios países tomaron como objetivo un sitio web delictivo que suministraba programas informáticos para que los delincuentes realizaran llamadas automáticas que simulaban ser servicios legítimos. Esto interrumpió el suministro de programas informáticos que, según las estimaciones, se utilizaron para realizar 10 millones de llamadas fraudulentas a ciudadanos y causaron pérdidas por valor de 115 millones de euros (Europol, "Online fraud schemes"). Véase también Alice Hutchings y Thomas Holt, "The online stolen data market: disruption and intervention approaches", *Global Crime*, vol. 18, núm. 1 (2016).

[306] Eva Nagyfejeo, "EU's emerging strategic cyber culture(s)", *Policing: A Journal of Policy and Practice*, vol. 15, núm. 1 (marzo de 2021).

[307] Por ejemplo, el Grupo de Acción Conjunta contra la Ciberdelincuencia de Europol coordina la actividad operacional para combatir el fraude transnacional en los pagos, y Eurojust facilita la prestación de asistencia jurídica y la cooperación entre los países miembros (Eurojust, "Actions across Europe against online fraud with cryptocurrencies", comunicado de prensa, 7 de noviembre de 2023). Véase también Red de Justicia de Asia Sudoriental, disponible en www.unodc.org/roseap/en/SEAJust/index.html.

[308] UNODC, INTERPOL y Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres (ONU-Mujeres), *Women in Law Enforcement in the ASEAN Region* (Bangkok, 2020).

[309] UNODC, *Issue Paper: Organized Crime and Gender.*

ESTUDIO DE CASO: ACUERDO REGIONAL PARA COMBATIR EL FRAUDE ORGANIZADO

China y la Asociación de Naciones de Asia Sudoriental, junto con la Oficina de las Naciones Unidas contra la Droga y el Delito, han desarrollado una estrategia transnacional para mejorar las respuestas nacionales, bilaterales y regionales a la trata de personas y las operaciones de casino y estafa. Un objetivo clave es aumentar la capacidad de los organismos encargados de hacer cumplir la ley y de los profesionales de la justicia penal para responder de forma amplia y coordinada. Se creó una red regional de puntos focales para contribuir al intercambio de información y a la coordinación de las investigaciones penales, así como para facilitar la respuesta oportuna a las solicitudes de asistencia de los países de la región. Además, la red sirve para fomentar la capacidad de sus miembros en lo relativo a las investigaciones sobre ciberdelincuencia, ciencia forense digital, tratamiento de pruebas digitales, activos virtuales e investigaciones financieras. También se ocupa de examinar y reforzar la aplicación de los marcos legislativos y de políticas para hacer frente a los delitos relacionados con las operaciones de casinos y estafas, y de mejorar la cooperación con el sector privado, los organismos regionales y la sociedad civil.

Fuente: UNODC, Oficina Regional para Asia Sudoriental y el Pacífico, "ASEAN member States and the People's Republic of China regional cooperation roadmap to address transnational organized crime and trafficking in persons associated with casinos and scam operations in South-East Asia" (Bangkok, 2023).

Actuación policial a partir de información de inteligencia

El fraude organizado suele traspasar las fronteras jurisdiccionales al reclutar a coautores dispersos geográficamente, dirigirse a víctimas de múltiples jurisdicciones y utilizar proveedores de tecnología que se encuentran en el extranjero. Es posible que el fraude organizado que está geográficamente disperso no se ajuste a las prioridades de la actividad policial de un territorio, que se centra en una agenda localizada más que en una transfronteriza y que está vinculada a jurisdicciones, datos y sistemas discretos y localizados. La visibilidad está supeditada a la adopción de una perspectiva nacional o internacional de la delincuencia. Además, no todos los fraudes son percibidos de forma aguda por cada una de las víctimas: el impacto es difuso, y solo cuando se considera en conjunto este delito se convierte en grave, por ejemplo, debido a que los autores perpetran grandes volúmenes de fraude, adquieren un producto del delito cuantioso o socavan la confianza y la integridad de los sistemas legítimos[310]. La capacidad de evaluar el daño en este contexto depende de la disponibilidad de información para conectar los delitos e identificar la delincuencia persistente y los riesgos asociados.

La identificación del fraude organizado se basa en la recopilación de conjuntos de datos y el análisis de las conexiones entre datos puntuales para extraer información de inteligencia sobre grupos delictivos organizados. Una sola víctima que denuncia un fraude puede tener un conocimiento limitado de los delincuentes y sus métodos; las pautas delictivas y los correspondientes riesgos de delincuencia organizada se detectan mediante procesos de análisis de datos para conectar delitos distintos y producir la información necesaria para una respuesta policial proactiva. Un modelo de actuación policial centrado exclusivamente en la realización de investigaciones penales reactivas de los delitos denunciados no suele pasar de lo superficial para abordar la trama fraudulenta subyacente, ya que el fraude organizado rara vez se pone de manifiesto a partir de una denuncia aislada de fraude.

[310] Levi, "Organized fraud and organizing frauds".

Protección de las personas afectadas por la delincuencia organizada

Quienes cometen fraude emplean técnicas de ingeniería social para explotar los factores psicológicos y de conducta humanos que hacen a las personas vulnerables al engaño y la manipulación[311]. Por consiguiente, la prevención eficaz de la delincuencia depende no solo de que se desarrollen sistemas más seguros, sino también de que se dote al público y a la comunidad empresarial de los conocimientos, la conciencia y las capacidades necesarias para defenderse del fraude. El fraude es muy diverso y evoluciona continuamente, y la eficacia de las campañas de educación y concienciación reside en que los mensajes públicos sean lo suficientemente sucintos y claros como para influir en los comportamientos y la vigilancia del público[312]. La eficacia también radica en la accesibilidad de dichas campañas, incluida la consideración de los diferentes idiomas empleados por grupos de población específicos y las medidas de accesibilidad para las personas con discapacidad. La vulnerabilidad suele estar relacionada con cada contexto en particular, por lo que es posible que la información pública tenga que formularse junto con las personas que se dedican a mercados o actividades concretas en los que existen riesgos y dirigirse a esas personas[313]. Además, la vulnerabilidad no es estática: varía en función de las circunstancias de la víctima y de los métodos específicos que emplean los estafadores. Por lo tanto, puede ser necesario que los mensajes de prevención lleguen a una persona o empresa en situación de riesgo en el momento adecuado[314].

La misma persona puede ser víctima de los mismos autores de fraude en múltiples ocasiones, como en algunos casos de fraude romántico y de inversión, mediante la captación o manipulación o debido a una vulnerabilidad personal[315]; estas personas pueden no reconocer que están siendo víctimas de un fraude y no denunciarlo a la policía. Las fuentes de información financiera y de otro tipo pueden ayudar a identificar a las víctimas en riesgo e impulsar respuestas proactivas de protección por parte de las entidades encargadas de hacer cumplir la ley y otras organizaciones de los sectores público y privado[316].

Promoción de las asociaciones y la cooperación

Reunión de datos a nivel nacional

La información sobre el fraude procede de diferentes fuentes y adopta diversas formas. Incluye informes sobre delitos e información recibida de ciudadanos, sociedades del sector privado y pequeñas empresas que han sido objeto de fraude o de intentos de fraude, informes e información de inteligencia recogidos por reguladores del sector público o el sector privado e informes recogidos por organizaciones de defensa del consumidor u otras fuentes. Los organismos encargados de hacer cumplir la ley no

[311] Brandon Atkins y Wilson Huang, "A study of social engineering in online frauds", *Open Journal of Social Sciences*, vol. 1, núm. 3 (agosto de 2013).

[312] Véase, por ejemplo, Comisión Europea, Centro de Conocimientos Antifraude, Biblioteca, Buenas prácticas, "#Fraudoff", disponible en el Centro de Conocimientos y Recursos Antifraude de los Fondos de la Unión Europea (https://antifraud-knowledge-centre.ec.europa.eu/); y Cassandra Cross y Michael Kelly, "The problem of 'white noise': examining current prevention approaches to online fraud", *Journal of Financial Crime*, vol. 23, núm. 4 (octubre de 2016).

[313] Por ejemplo, la Comisión del Mercado de Valores de los Estados Unidos imparte formación específica a los futuros inversionistas para mejorar sus conocimientos del mercado y ayudarlos a defenderse del fraude (véase https://www.investor.gov/informacion-en-espanol).

[314] El objetivo de la Asociación de Intercambio de Información sobre Ciberseguridad (Cyber Security Information Sharing Partnership) del Reino Unido es ayudar a las empresas a compartir de forma segura información en tiempo real sobre ciberamenazas dinámicas, garantizando así que las organizaciones miembros sean conscientes de los riesgos emergentes y puedan aplicar contramedidas (Reino Unido, "Government launches information sharing partnership on cyber security", comunicado de prensa, 27 de marzo de 2013).

[315] Véase, por ejemplo, Elisabeth Carter, "Confirm not command: examining fraudsters' use of language to compel victim compliance in their own exploitation", *The British Journal of Criminology*, vol. 63, núm. 6 (noviembre de 2023).

[316] En Australia, por ejemplo, la policía, en colaboración con el departamento de comercio del gobierno, supervisa las transferencias internacionales de dinero a países de alto riesgo para identificar e implicar a las personas sospechosas de ser víctimas de fraude (Cross y Blackshaw, "Improving the police response to online fraud").

tienen el monopolio de los datos sobre fraude y esta diversidad de fuentes dificulta la elaboración de un panorama completo de la delincuencia que demuestre la magnitud y la naturaleza del problema[317]. La fragmentación de los datos supone un reto para los organismos estatales a la hora de identificar y rastrear modalidades y tendencias clave, evaluar riesgos, asignar funciones y recursos y desarrollar estrategias sólidas. También se carece de datos desglosados por género sobre esta cuestión, lo que afecta a la capacidad de las autoridades nacionales para comprender las tendencias de género y las características interrelacionadas que conforman las experiencias de las personas con el fraude organizado. Sin embargo, hay una serie de medidas que pueden adoptarse para obtener una imagen más consolidada. Estas medidas se describen a continuación.

Centralización de las denuncias de fraudes

La fragmentación de las posibilidades de denuncia puede repercutir en las víctimas y en su experiencia a la hora de buscar la ayuda y el apoyo que necesitan. Pueden encontrarse con un panorama desconcertante de entidades de los sectores público y privado y organizaciones de la sociedad civil que ofrecen una amplia diversidad de posibilidades de apoyo, y encontrar el servicio adecuado puede implicar un prolongado proceso de ensayo y error, en el que las víctimas son transferidas de una organización a otra[318]. Este problema puede verse agravado por la debilidad de las respuestas policiales, especialmente en los equipos regionalizados que tienen una capacidad limitada para emprender investigaciones complejas y transfronterizas. La existencia de canales de denuncia ágiles y conectados entre sí contribuye a garantizar que las víctimas reciban el apoyo que necesitan, al tiempo que se consolida el panorama nacional sobre el fraude y sus víctimas.

ESTUDIO DE CASO: DENUNCIAS CENTRALIZADAS

En Australia, el Centro Nacional contra las Estafas es un ejemplo de iniciativa gubernamental para facilitar a las víctimas la denuncia del fraude. Este organismo se centra en la protección del consumidor y adopta el principio de "ninguna puerta equivocada", según el cual, independientemente de las circunstancias y necesidades individuales, todas las víctimas de fraude reciben apoyo. En otros países se ha hecho hincapié en la consolidación de los sistemas de registro de delitos mediante la creación de centros nacionales de denuncia para las víctimas del fraude y la ciberdelincuencia. Por ejemplo, en los Estados Unidos de América, el Centro de Denuncias de Delitos Cometidos en Internet, gestionado por el Buró Federal de Investigaciones, recibe todas las denuncias públicas de delitos cometidos en Internet, incluido el fraude.

Fuentes: Australia, National Anti-Scam Centre, "National Anti-Scam Centre in action", actualización trimestral (julio-septiembre de 2023); y www.fbi.gov/video-repository/ic3_112117.mp4/view.

La disponibilidad de un único organismo responsable y fidedigno para recibir las denuncias de delitos facilita el proceso para las víctimas, lo que es especialmente importante en el fraude si se tiene en cuenta la gran cantidad de casos que no se denuncian[319].

[317] Levi y Burrows, "Measuring the impact of fraud in the UK".

[318] Button *et al.*, "Not a victimless crime".

[319] Por ejemplo, solo el 17 % del fraude experimentado por el público en el Reino Unido en el período de 12 meses comprendido entre abril de 2016 y marzo de 2017 fue denunciado a la policía (Reino Unido, Ministerio del Interior, *The Scale and Nature of Fraud: A Review of the Evidence* (2018)).

Integración de conjuntos de datos

Para luchar contra el fraude, es indispensable establecer asociaciones estratégicas con el sector privado y otras partes interesadas, entre otras cosas con el fin de desarrollar marcos jurídicos para intercambiar datos e información sobre la delincuencia. Un alto volumen de fraude se dirige a instituciones como bancos, otros proveedores de servicios financieros, comercio electrónico y otras empresas. Esto se hace a menudo mediante cuentas legítimas de clientes (p. ej., toma de cuentas o fraude al consumidor), y muchas víctimas individuales denuncian este tipo de fraude a su proveedor de servicios en lugar de a la policía. Además, las empresas del sector privado realizan complejos análisis de datos para identificar riesgos y defenderse del fraude, o incluso pueden iniciar sus propias investigaciones internas para identificar a los autores. Se necesitan cauces para garantizar que estos datos puedan compartirse fácilmente con las entidades encargadas de hacer cumplir la ley u otros organismos públicos[320].

Integrar conjuntos de datos de distintos sectores ayuda a obtener una imagen estratégica más completa del problema. Esta información compartida también puede utilizarse para impulsar respuestas tácticas a la delincuencia y a los riesgos relacionados con ella que, de otro modo, podrían permanecer ocultos. Estas respuestas incluyen actividades dirigidas a hacer cumplir la ley basadas en la inteligencia e intervenciones de reducción de daños para señalar los riesgos y proteger a las personas o empresas de convertirse en víctimas de fraudes.

Alianzas entre los sectores público y privado

El fraude organizado rara vez tiene lugar en los espacios públicos que están bajo el control del Estado, sino que se hace presente más bien en espacios que están bajo el control comercial de intermediarios del sector privado que proporcionan comunicaciones basadas en Internet, comercio electrónico, servicios financieros, aplicaciones web y telecomunicaciones. Las empresas del sector privado diseñan las tecnologías y los sistemas que los delincuentes incorporan y explotan como parte de esquemas fraudulentos. También son fundamentales como víctimas, proveedores de seguridad en línea, fuentes de información para comprender este tipo de delitos y centros de conocimientos especializados y capacidad en la lucha contra el fraude. Tienen un papel especialmente importante en la formulación y la aplicación de estrategias que eliminen las vulnerabilidades de los sistemas que aprovechan los delincuentes, con vistas a mitigar futuros riesgos de fraude organizado. El alcance de la lucha contra el fraude organizado depende del fomento de la cooperación con las empresas del sector privado que, individual y colectivamente, rigen los dominios digitales que constituyen un terreno fértil para el fraude.

La capacidad de los intermediarios del sector privado para actuar contra quienes cometen actos de fraude organizado será diferente según sus funciones y lo directa que sea su relación comercial con la persona que utiliza sus servicios con fines delictivos. En virtud de los principios estratégicos de fomento de la cooperación y las alianzas en un enfoque de toda la sociedad para hacer frente a la delincuencia organizada, los intermediarios del sector privado pueden adoptar una serie de funciones clave[321], entre las que se cuentan las siguientes:

- Identificar a los presuntos autores y actividades delictivas y notificarlo a las autoridades o a las víctimas previstas (incluida la denuncia de irregularidades en relación con fraudes internos)
- Impedir que las comunicaciones fraudulentas lleguen a las víctimas, por ejemplo, eliminando o bloqueando sitios web, anuncios o perfiles maliciosos

[320] En el Reino Unido, la policía ha desarrollado una estrecha colaboración con Cifas y United Kingdom Finance, que recopilan datos sobre el fraude dirigido a sus organizaciones miembros, entre las que se encuentran los principales interesados en los servicios financieros. Véase, por ejemplo, Reino Unido, Oficina de Estadísticas Nacionales, "Crime in England and Wales: year ending June 2023", 19 de octubre de 2023.

[321] UNODC, *Guía práctica para elaborar estrategias de alto impacto contra la delincuencia organizada.*

- Proporcionar datos desglosados por género para mejorar el panorama estratégico de inteligencia y facilitar las investigaciones de delitos
- Evitar la pérdida de fondos transferidos a delincuentes
- Educar a los usuarios de sus servicios sobre el fraude y concienciarlos de forma accesible y adaptada a los distintos grupos destinatarios
- Elaborar sistemas y políticas que minimicen y mitiguen el riesgo de fraude

En los casos en que el fraude representa una amenaza para una empresa o un sector, las estrategias pueden guiarse por necesidades y objetivos interiorizados[322]. En algunos casos, los sistemas de distintos sectores o empresas pueden servir de conducto para fraudes que repercuten en agentes u organismos externos, como miembros del público u otros sectores. Por ejemplo, el uso de las telecomunicaciones para enviar mensajes de texto fraudulentos es un tipo de fraude que sufren las víctimas individuales y los proveedores de servicios financieros que procesan los pagos o las solicitudes de transferencia.

Adoptar una perspectiva estratégica en diversos sectores facilita la identificación de las vulnerabilidades de todo el sistema en la infraestructura tecnológica, comercial o financiera. Una forma de hacerlo consiste en examinar estratégicamente las etapas clave de la comisión de determinados tipos de fraude y definir las convergencias con las tecnologías, los productos y los servicios, incluidos, por ejemplo, el canal de entrada para establecer el contacto inicial con las víctimas (p. ej., anuncios en las redes sociales), la interacción con las víctimas (p. ej., mensajes falsificados) y los procesos de cobro para acceder al producto del delito (p. ej., sistemas de pago).

La coordinación debe realizarse de forma que tenga en cuenta el abanico de industrias y organizaciones que componen esta infraestructura, incluidas las sociedades comerciales de alcance mundial y las empresas más pequeñas, las empresas ubicadas dentro del país y las que operan fuera de la jurisdicción legal, y las empresas con acceso a diversos recursos y capacidades para ayudar en la labor de lucha contra el fraude[323]. Existen diferentes formas de incorporar al sector privado a un planteamiento coordinado, entre los que se incluyen el fomento de asociaciones estratégicas entre el Estado y el sector privado y las organizaciones de la sociedad civil[324], el establecimiento y acuerdo de normas o principios voluntarios que ayuden a dirigir políticas y prácticas más coherentes en las distintas empresas, y el establecimiento de normativas legales para imponer obligaciones a las principales partes interesadas del sector privado[325].

Es importante desglosar las etapas clave del fraude a fin de contribuir a definir los puntos estratégicos relevantes para orientar la actividad de prevención de la delincuencia. Existen múltiples ejemplos de establecimiento de alianzas público-privadas con el fin de aplicar estrategias de prevención de la vulnerabilidad sistémica. Los estudios de casos que se exponen a continuación representan iniciativas dirigidas a hacer frente a cada una de las etapas del fraude descritas anteriormente.

[322] Por ejemplo, el Servicio de Prevención del Fraude de África Meridional (Southern African Fraud Prevention Service) facilita el intercambio de información entre las empresas asociadas para detectar y abordar los riesgos internos de fraude (véase www.safps.org.za/Home/About).

[323] Véase, por ejemplo, Michael Levi y Matthew Leighton Williams, "Multi-agency partnerships in cybercrime reduction: mapping the UK information assurance network cooperation space", *Information Management and Computer Security*, vol. 21, núm. 5 (noviembre de 2013).

[324] Véase, por ejemplo, Reino Unido, Ministerio del Interior, "Joint fraud taskforce", 17 de octubre de 2017.

[325] Por ejemplo, la Ley de Servicios Digitales de la Unión Europea introducirá nuevas obligaciones para que los mercados en línea rastreen a los vendedores en su plataforma para ayudar a perseguir con mayor eficacia a quienes cometen fraude. Véase https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.

ESTUDIO DE CASO: RESPUESTA INTERSECTORIAL A SITIOS WEB MALICIOSOS

El Centro Nacional de Ciberseguridad del Reino Unido de Gran Bretaña e Irlanda del Norte ha concertado acuerdos con proveedores de servicios de Internet en el Reino Unido para transmitir información en tiempo real sobre sitios web que han sido identificados como fraudulentos. Los proveedores pueden entonces bloquear el acceso a los sitios web fraudulentos e impedir que los estafadores asociados a ellos se comuniquen con posibles víctimas en el Reino Unido.

Fuente: Reino Unido, Centro Nacional de Ciberseguridad, "NCSC joins industry to offer unprecedented protection for public from scams", 11 de mayo de 2022.

ESTUDIO DE CASO: RESPUESTA INTERSECTORIAL A LA COMUNICACIÓN MASIVA POR MENSAJE DE TEXTO

En un intento de frenar el elevado volumen de *smishing*, práctica en la que los delincuentes sacan partido de las telecomunicaciones para hacerse pasar por organizaciones legítimas, la Autoridad Australiana de Comunicaciones y Medios de Información ha establecido un registro de remitentes de mensajes de texto. El sistema fomenta la participación de las principales partes interesadas del sector para establecer un directorio de remitentes de confianza con el fin de restringir la capacidad de los delincuentes para enviar mensajes de texto masivos que suplanten la identidad de estas organizaciones. Esto serviría para filtrar los mensajes maliciosos que fingen provenir de estas organizaciones y evitar así que lleguen a posibles víctimas

Fuente: Parlamento de Australia, "Telecommunications Amendment (SMS Sender ID Register) Bill 2024", disponible en www.aph.gov.au/.

ESTUDIO DE CASO: CENTRO INTERSECTORIAL PARA PREVENIR LA PÉRDIDA DE DINERO POR FRAUDE

En Singapur, el Mando Antiestafas es una unidad policial centralizada que ha forjado estrechas alianzas con una serie de proveedores de servicios financieros, algunos de los cuales comparten locales con ella. Entre las partes interesadas figuran bancos locales y extranjeros, grupos de seguridad de tarjetas, empresas de tecnología financiera y casas de criptomonedas. Este enfoque integrado permite compartir rápidamente información y analizar la inteligencia financiera para detectar y bloquear transferencias financieras sospechosas de ser fraudulentas. Los pagos en línea y las transferencias bancarias permiten a quienes cometen fraude mover y cobrar rápidamente los fondos robados, y el objetivo de esta colaboración es congelar con celeridad las cuentas, recuperar los fondos y reducir así las pérdidas de las víctimas.

Fuente: Policía de Singapur, "Opening of anti-scam command office", 6 de septiembre de 2022.

Las respuestas eficaces al fraude también deben tener en cuenta el panorama normativo en relación con el suministro de productos y servicios. La accesibilidad de estos productos y servicios proporciona el camuflaje para ocultar tramas fraudulentas y engañar a las víctimas. La regulación desempeña un papel clave en la aplicación de mecanismos de confianza eficaces para evitar que los agentes maliciosos operen desde sectores legítimos. Esto incluye adoptar principios sólidos de conocimiento de los clientes para los

reguladores de los sectores público y privado a la hora de abrir cuentas bancarias, solicitar el uso de otros servicios habilitadores como servicios de pago, telecomunicaciones y otros servicios empresariales (p. ej., alquiler de oficinas) y registrar empresas o profesionales (p. ej., profesionales de servicios financieros).

Los delitos que engloba el fraude organizado atraviesan fronteras nacionales, sectores y grupos demográficos. Esto complica la elaboración de políticas y la aplicación de respuestas eficaces. Hay pasos fundamentales que cada Estado puede dar, en primer lugar, para comprender cómo se manifiesta el fraude organizado y cómo repercute dentro de sus fronteras y, en segundo lugar, para formular y aplicar respuestas estratégicas eficaces en los cuatro pilares de la lucha contra la delincuencia organizada (prevenir, perseguir, proteger y promover). La formulación de políticas también debe tener en cuenta el contexto transnacional del fraude organizado para garantizar la aplicación de respuestas internacionales coordinadas. Además, el fraude organizado exige una respuesta de toda la sociedad que incorpore asociaciones estratégicas con las principales partes interesadas no gubernamentales, especialmente en el sector privado, para lograr una mejor comprensión del problema y elaborar estrategias para combatirlo.

Conclusión

El fraude organizado representa una amenaza polifacética y omnipresente que trasciende fronteras, sectores y grupos demográficos. Para abordar esta compleja cuestión se necesita un enfoque integral, empezando por el desarrollo de un lenguaje y una comprensión comunes respecto de las diferentes categorías de fraude organizado.

Este documento temático tiene por objetivo contribuir al conocimiento académico mediante una perspectiva general del fraude organizado dirigido contra particulares o instituciones privadas con el fin de obtener un beneficio económico u otro beneficio de orden material. Las categorías de fraude aquí descritas adoptan una perspectiva centrada en la víctima y, por tanto, se focalizan principalmente en la narrativa o artimaña que se presenta a las víctimas. El documento temático, aunque amplio, no es exhaustivo, y sigue habiendo gran cantidad de posibles cuestiones pertinentes en relación con el fraude organizado. Se necesita más investigación por parte de académicos, profesionales y la sociedad civil para desarrollar nuestro conocimiento y comprensión de un ámbito de la delincuencia muy diverso y complejo.

Las categorías de fraude organizado presentadas en el documento temático tienen por objeto proporcionar a las partes interesadas una mejor comprensión de la cuestión, con vistas a fomentar estrategias eficaces de múltiples partes interesadas para prevenir el fraude organizado, perseguir a los grupos delictivos organizados, proteger a las personas afectadas por el fraude organizado y promover las asociaciones y la cooperación, así como salvaguardar a las víctimas y aumentar la resiliencia de la sociedad frente a esta persistente amenaza. La colaboración entre sectores, la innovación continua y el compromiso inquebrantable con la defensa de la justicia y los derechos humanos son esenciales para mitigar el impacto del fraude organizado y promover un entorno mundial más seguro.

No obstante, aún queda mucho por hacer. El documento temático sobre el fraude organizado forma parte de un proyecto más amplio que desarrollará herramientas e investigaciones adicionales para prevenir y combatir el fraude organizado, incluidas medidas para reforzar la legislación, aumentar la conciencia y las defensas en la población y fomentar una cooperación eficaz con el sector privado y otros sectores, entre otras cosas. Si se sigue avanzando en el conocimiento y la capacidad de respuesta, se podrán lograr avances significativos en la protección de particulares e instituciones frente a la amenaza omnipresente del fraude organizado.

UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0; fax: (+43-1) 263-3389; www.unodc.org

2412213