CPA PANAMÁ Vol.4, No.1 enero-junio 2026 ISSN-L 2953-3147
pp.114-135

Delitos financieros digitales en la era de la hipervigilancia

Digital financial crimes in the era of hyper-surveillance

Andrés Ahumada Aranda
Universidad de Panamá, Panamá
https://orcid.org/0009-0007-4918-150X
andrésahumadaaranda@gmail.com

Fecha de recibido: 31 de octubre de 2025
Fecha de aceptación: 1 de diciembre de 2025

DOI https://doi.org/10.48204/2953-3147.8573

Resumen

Esta investigación, de corte documental y exploratorio, se propuso entender un fenómeno que crece más rápido que las leyes: los delitos financieros digitales en Panamá entre 2020 y 2025. El objetivo fue mirar más allá de las cifras, detenerse en las definiciones que la doctrina y los informes técnicos ofrecen, y ponerlas en diálogo con la realidad que viven instituciones, empresas y ciudadanos en el espacio digital. El estudio se apoyó en un enfoque cualitativo y reflexivo. Se revisaron leyes nacionales, informes internacionales, artículos académicos y registros de incidentes cibernéticos. Más que buscar una verdad definitiva, se trató de comprender cómo interactúan las dimensiones tecnológicas, legales y sociales en la expansión del cibercrimen. Los resultados muestran un crecimiento sostenido de ataques como el *ransomware*, el *phishing* y los fraudes en línea. También revelan un desfase

preocupante, mientras la tecnología avanza exponencialmente, la respuesta penal se mueve a ritmo lento. Sin embargo, la promulgación de la Ley 478 de 2025 y la inminente adhesión al Convenio de Budapest marca un paso firme hacia una persecución más efectiva del delito digital. En conclusión, el país avanza, pero todavía queda mucho por afinar. Es urgente fortalecer la norma penal, formar especialistas en el sistema judicial y, sobre todo, repensar el equilibrio entre vigilancia y privacidad. Porque cada avance tecnológico, sin ética ni control, corre el riesgo de convertirse en una nueva forma de vulnerabilidad humana.

Palabras clave: fraude, delito informático, tecnología digital, redes sociales.

Abstract

This documentary and exploratory research set out to understand a phenomenon that evolves faster than the law itself: digital financial crimes in Panama between 2020 and 2025. The objective was to look beyond statistics, to pause on the definitions proposed by doctrine and technical reports, and to place them in dialogue with the lived realities of institutions, businesses, and citizens in the digital sphere. The study relied on a qualitative and reflective approach. It reviewed national legislation, international reports, academic literature, and records of cyber incidents. Rather than seeking a definitive truth, it aimed to understand how technological, legal, and social dimensions intertwine in the expansion of cybercrime. The results reveal a steady rise in attacks such as ransomware, phishing, and online fraud, as well as a troubling gap: while technology advances exponentially, legal responses move at a much slower pace. However, the enactment of Law 478 of 2025 and the forthcoming ratification of the Budapest Convention represent a firm step toward a more effective prosecution of digital crimes. In conclusion, the country is making progress, yet much remains to be refined. Strengthening criminal law, training

judicial specialists, and—above all—rethinking the balance between surveillance and privacy are urgent needs. Every technological advance, without ethics or oversight, risks becoming a new form of human vulnerability.

Key words: fraud, computer crime, digital technology, social network.

Introducción

Esta investigación, de carácter documental y exploratorio, tiene como propósito examinar las principales definiciones asociadas a los delitos financieros digitales, mediante el análisis de artículos académicos, doctrina jurídica y publicaciones especializadas que abordan el uso de herramientas tecnológicas y digitales. Además, el estudio busca integrar los aportes de diversos investigadores con el fin de alcanzar una comprensión más profunda del fenómeno desde una perspectiva jurídica.

Metodología

La investigación se desarrolló bajo un enfoque reflexivo y cualitativo, porque lo que se busca es comprender el fenómeno más allá de las estadísticas. Este enfoque permitió analizar el fenómeno de los delitos financieros digitales en Panamá no como una simple acumulación de datos, sino como es en las prácticas, y la interacción con las normas penales.

El diseño fue exploratorio-descriptivo, ya que el objetivo principal consistió en identificar y caracterizar las manifestaciones recientes de este tipo de delitos, así como las respuestas institucionales y legales que han intentado contenerlos. Según Hernández Sampieri, Fernández y Baptista (2014), el enfoque cualitativo

exploratorio-descriptivo permite aproximarse a fenómenos poco estudiados o en transformación, favoreciendo la interpretación contextual antes que la generalización estadística.

Para ello, se revisaron leyes vigentes, informes internacionales y nacionales, así como literatura académica especializada. Además, se incorporó el análisis de casos documentados entre 2020 y 2025 que ilustran la evolución del delito financiero digital en Panamá.

Resultados y discusión

Miró Llinares (2018) nos da un enfoque sobre el ciberdelito cuando se refiere a que:

> En los últimos tiempos se ha venido sustituyendo, aunque no por todos, la denominación de delitos informáticos por la de cibercrimen y cibercriminalidad en referencia esta vez al termino anglosajón *cybercrime*, procedente de la unión entre el prefijo *cyber*, derivado del término *cyberspace*, y el termino *crime*, como concepto que sirve para englobar la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio. (p. 36).

A pesar de que existen muchas concepciones al respecto, este autor genera aportes conceptuales que nos permite examinar la realidad social vinculada a estos delitos financieros y digitales, a partir de sus reflexiones acerca del ciberespacio y como es que a través de esta brecha es aprovechada y operan los ciberdelincuentes, nos permite un acercamiento al conocimiento de este fenómeno

También considera que, aunque hay múltiples definiciones de cibercrimen, el aspecto esencial de todas y cada una de ellas se reduce, y como ya se ha adelantado, a la cuestión de si con la definición se está adoptando una concepción

amplia o restringida de la cibercriminalidad, dando cobertura en la categoría a todos o tan solo a algunos de los comportamientos criminales realizados en el ciberespacio.

Nava Garces (2017) en un pasado reciente dio su opinión en entrevista para un canal del Instituto Nacional de Investigaciones Penales, en Ciudad de México, Respecto a las diferencias entre delito informático, tecnológico y ciberdelito. Una explicación muy acorde a nuestra realidad y detalló como opera cada tipo de delito y sus variantes y dejó ver la complejidad y el crecimiento de este tipo de delitos.

Ante estas circunstancias no es posible contar en este momento con normativas desde el punto de vista penal que vayan a la par del desarrollo tecnológico y todo lo que con ello se genera, es decir, el crecimiento de ataques al sistema financiero es abrumador y exponencialmente peligroso para cualquier Estado en el mundo. Sin embargo, hay que considerar que el Estado panameño ha dado pasos que apuntan hacia la dirección correcta.

Es notorio que el sistema judicial, al igual que todos los que hacen uso de este, enfrenta vacíos legales e incertidumbres. Se considera que corresponde al Estado ofrecer respuestas efectivas frente a dichas circunstancias, las cuales generan en la sociedad descontento, y una creciente falta de credibilidad en las instituciones, tanto públicas como privadas, entre ellas la fiscalía, policía y el sector bancario.

Por estas razones, se valoran positivamente las actualizaciones que recientemente se implementaron, hay que decir, que es solo el inicio de un esfuerzo orientado a fortalecer la respuesta estatal y reducir los indicadores negativos que actualmente se observan.

Según los datos del Instituto Nacional de Ciberseguridad (INCIBE-Ciberseguridad, 2024), Entre los incidentes más recurrentes destacaron:

- *Malware*, con **42.136 casos**, incluyendo virus y otros softwares maliciosos que afectan dispositivos. De estos, **357** fueron ataques de *ransomware*, donde los ciberdelincuentes bloquean sistemas o archivos, exigiendo rescates económicos.
- Fraude *online*, con más de **38.000** incidentes, representando el 43,2% del total. El *phishing* lidera esta categoría con **21.571** casos, como correos falsos simulando ser bancos o empresas conocidas para robar datos personales.
- Se identificaron **7.470** intrusiones e intentos de acceso no autorizados a información de redes o sistemas informáticos de empresas y hogares, como el hackeo de una red doméstica que expone datos familiares.
- Se gestionaron **2.122** incidentes de tiendas *online* fraudulentas, afectando a consumidores engañados por plataformas falsas.

Por supuesto que esto hace que se convierta en un verdadero problema para cualquier Gobierno, pues al verse atacado por ciberdelincuentes en su estructura financiera pública como privada, no queda más, que tratar de mitigar con las herramientas a su alcance, esa realidad que azota a la sociedad día y noche, como si fuera un ejército de personas tratando de penetrar cualquier rincón posible de nuestros datos privados, usando, phishing, malware, ransomware y la denominada ingeniera social, el gran desafío es frenar el daño económico que generan a la estructura financiera local, regional y global. ¿la gran incógnita es como hacerlo?

En los últimos años, el cibercrimen desarrolló un talento que muchos empresarios envidiarían, siempre encuentra cómo reinventarse. Hace algunos años sucedía como en las películas de vaqueros cuando los asaltantes con sombrero y

pistola, se escondían siempre por caminos polvorientos y lejos de cualquier poblado y del Sherif lógicamente. Hoy, los nuevos ciberdelincuentes no ensucian sus botas, crean algoritmos y manipulan billeteras digitales. Los delitos financieros digitales crecen igual y al mismo ritmo que las criptomonedas y las aplicaciones de pago, mientras los sistemas judiciales del mundo corren como atletas sobre sillas de ruedas y además pareciera que avanzan sobre piedras, intentando alcanzar a un enemigo que ya va en un avión privado.

Por increíble que parezca hasta en restaurantes puede estar clonado el QR utilizado para consultar el menú, así de rápido pueden obtener nuestros datos de contacto en nuestro teléfono celular, y más crítico aún, si contiene su tarjeta bancaria digital dentro del mismo celular, o la banca en línea, por ejemplo, incluso muchos profesionales guardan presentaciones profesionales, planos de diseño arquitectónico, por solo mencionar algunos.

Según el estudio realizado por la ONU (2022), El *hacking* es un término que se utiliza para definir el acceso no autorizado a los sistemas, redes, y datos (en adelante, objetivos). Es posible que el *hacking* se perpetre solo para tener acceso a un objetivo o ganar o mantener tal acceso más allá de la autorización. Este término que se lee tan fácil, por supuesto denota una complejidad para todos aquellos no familiarizados con tecnología, internet y redes sociales, porque ese desconocimiento es aprovechado por ciberdelincuentes, y organizaciones criminales bien estructuradas, en muchos caso con tintes internacionales, que en un santiamén pueden dejar vacía una cuenta de ahorros de una persona, se hace mención de personas por ser la parte más débil además de contar con menos recursos para impedir que eso suceda. Pero puede ocurrirle a cualquiera, el crecimiento de estafas y fraudes digitales explotó.

Cuando el mundo entero se convirtió en un silencio abrumador, donde nuestras salas de estar era el lugar de reunión, de juegos, de ver noticias, además donde las familias se reunían en cocinas improvisadas como oficinas y pantallas de computadoras eternamente encendidas, algo más que el virus se esparció con sigilo cuidadosamente planeado, el cibercrimen.

Con el surgimiento del COVID-19 y el consecuente confinamiento de cientos de millones de personas, la vida cotidiana se digitalizó a una velocidad que habría enrojecido de envidia a cualquier tecnócrata de Silicon Valley. Comprar, transferir, firmar documentos, hacer filas (ahora virtuales) … todo se trasladó al universo intangible de lo digital, ese espacio que promete comodidad mientras absorbe, sin hacer ruido, datos personales, contraseñas y secretos financieros.

Según Díaz (2021) en un informe avalado por la Comisión Económica para América Latina y el Caribe (CEPAL), la situación de la ciberseguridad en la logística de América Latina y el Caribe durante la pandemia fue, por decirlo suavemente, es preocupante. Mientras la economía global se desplomaba, el crimen digital vivía su propio auge, más sofisticado, más organizado, más rentable.

El mismo fenómeno que llevó a las universidades a descubrir el Zoom y a las personas a usar WhatsApp, permitió a los delincuentes digitales con la ayuda del aprendizaje automático “machine learning”, por sus siglas en inglés y la inteligencia artificial desarrollar ataques cada vez más precisos, como si el caos mundial les hubiera ofrecido, el laboratorio perfecto para sus experimentos.

Por si fuera poco, la “Deep web” o “web profunda” ese inframundo del internet se convirtió en un supermercado del delito. Sin restricciones allí se ofrece malware, además de páginas web, una modalidad tan profesionalizada que una persona promedio no imagina.

Díaz (2021) señala además que," mientras tanto, el tráfico en internet creció un 1,5% anual y las transacciones digitales se dispararon un 26,7%. Es decir: cada vez más gente haciendo más cosas en un lugar donde la ley es borrosa y la policía, inexistente. Como mudarse a una ciudad sin semáforos, convencidos de que nadie va a acelerar." (p. 8)

Así, en esta paradoja contemporánea, el confinamiento transformo la dinámica social, laboral, educativa, y derivo en la posibilidad de acceder a una exposición digital sin precedentes. El hogar, refugio tradicional frente al caos del mundo, se volvió la puerta de entrada a un nuevo tipo de vulnerabilidad silenciosa, invisible, pero profundamente invasiva.

Antes de toda esta cuestión financiera digital, el contraste resulta difícil de asimilar desde una perspectiva racional. Antes, el dinero era un objeto palpable, billetes arrugados que podían verse, y monedas cuyo sonido metálico recordaba lo material del intercambio. Hoy, las transacciones son inmateriales, pero paradójicamente dejan rastros mucho más nítidos, nuestros datos personales, esa moneda tan valiosa como el oro, que las instituciones financieras dicen custodiar hasta que un hacker, con menos esfuerzo que un carterista de antes, se los arrebata.

Frente a estas circunstancias, la vigilancia tecnológica se ofrece como una solución. Se nos promete seguridad, rapidez y modernidad. Pero como todo remedio milagroso, trae efectos secundarios difíciles de ignorar, videovigilancia que observan desde las esquinas, micrófonos que escuchan desde los aparatos que compran "para facilitarnos la vida", y algoritmos que conocen nuestras rutinas con una exactitud e intimidad.

La pregunta se impone sola. ¿en qué momento dejamos de ser ciudadanos y pasamos a ser ciudadanos observados por alguien que parece invisible?

La llamada “cuarta revolución industrial” donde las reglas y los algoritmos ha traído consigo un tipo de criminalidad tan intangible como omnipresente. Los delitos financieros digitales no es un grupo para asaltar bancos. Mientras las monedas físicas se evaporan en la nube y las fintech prometen democratizar el dinero, emergen los algoritmos, donde las leyes aún no han determinado los límites del poder ni de la culpa.

En este escenario, la “era de la hipervigilancia”, cámaras invisibles rastrean patrones de consumo, inteligencias artificiales perfilan victimas antes de que cometan un error y los mercados financieros se conviertan en una huella jurídica. Cuanto más intentamos asegurar el sistema, más lo exponemos al control.

Los esfuerzos internacionales, las criptomonedas y la blockchain, nacidas con la promesa de la descentralización, se convierten a veces en refugio para la opacidad. Y mientras los Estados persiguen delitos que ya no tienen rostro ni domicilio, el Derecho Penal diseñado para perseguir delitos tangibles y además en su territorio, no persiguen en el ciberespacio, se requieren participación de otros Estados.

Desde una mirada crítica, este debate no es solo técnico, sino moral: ¿hasta dónde puede llegar el poder punitivo en nombre de la seguridad? ¿Cuánta libertad estamos dispuestos a sacrificar en aras de la trazabilidad? La vigilancia algorítmica reconfigura el principio de proporcionalidad, castigar ya no es solo sancionar, sino también prever, anticipar, prevenir. El riesgo es que, en nombre del orden digital, terminemos aceptando una justicia predictiva que trate a los ciudadanos como potenciales sospechosos permanentes.

Este trabajo, por tanto, no pretende añadir otra capa de regulación, sino más bien abrir un espacio de reflexión. Una justicia penal digital verdaderamente garantista debe combinar precisión tecnológica con prudencia humanista,

algoritmos sí, solo así el Derecho podrá sobrevivir a los cambios que lo amenaza muy de cerca.

Vivimos en una era de avances tecnológicos tan vertiginosos que lo imposible de ayer es la aplicación gratuita de hoy. Sin embargo, bajo el tamiz de la innovación, vive una paradoja incómoda, cuanto más conectada está la sociedad, más expuesta queda, las interioridades de cualquier ciudadano, empresa o institución pública, puede ser observada, pueden escanear información sensitiva.

El mundo actual hiperconectado, globalizado, digitalizado, no solo ha acortado distancias, sino también ha facilitado que el delito este presente cotidianamente. El crimen ya no necesita pasaporte basta dar clic. En esta, denominada aldea global, los delincuentes digitales operan con impunidad, porque se mantienen en el anonimato. Y los estados, con sus leyes aún redactadas en un lenguaje analógico, van detrás porque les resulta imposible estar al mismo nivel que la ciberdelincuencia.

Estamos, pues, ante un nuevo horizonte de conflicto, el ciberespacio. Aquí no bastan jueces ni códigos; hacen falta alianzas transnacionales, marcos legales flexibles y, sobre todo, una comprensión profunda de que el poder ya no solo se ejerce desde la asamblea legislativa, sino también desde los teclados.

Como expresa Miró Linares (2012),

> Si utilizamos el término de forma amplia, podremos definir como *cibercrimen* cualquier conducta delictiva en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes

sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet. (p. 42).

En relación a lo expresado por Miró, es importante recalcar que actualmente las tecnologías de la información, en esencia permanece la acepción, sin embargo, es necesario decir que todo lo que circule por esta vía, como mensajes de texto, correos, voz, video, datos, imágenes, etc. Su evolución y transformación sigue desarrollándose cada vez más, provoca con ello que surjan nuevos conceptos, que bien pueden quedar contenidos en la concepción inicial de Miró.

Para examinar la realidad respecto a estos fenómenos delictivos en Panamá, se puede decir que, el Código Penal sanciona el acceso indebido a sistemas informáticos y la manipulación de datos, pero por la naturaleza transnacional de estos delitos exige cooperación internacional. En ese sentido, la adhesión de Panamá al Convenio de Budapest en 2013 (Ley 79 de 2013) refleja el reconocimiento de esta necesidad. Mientras los ciberdelincuentes afinan sus tácticas con algoritmos de última generación, muchos códigos penales de otras naciones siguen anclados en lógicas del siglo XX. En el caso particular de Panamá, los marcos jurídicos de 1982 y 2007, que alguna vez parecieron modernos, hoy resultan tan insuficientes para intentar frenar un ciberataque.

Estos textos legales, nacidos en épocas donde los delitos aún dejaban huellas físicas como una cerradura forzada, una carta falsificada, un arma, actualmente no logran captar la naturaleza intangible, ubicua y mutante de la criminalidad digital. Robar una identidad virtual, vulnerar una base de datos o encriptar sistemas enteros para exigir rescate son acciones que escapan a las categorías tradicionales de lo punible. Sin categorías claras, y operadores sumamente calificados no hay protección posible.

Esto revela un desfase alarmante, los bienes jurídicos, la intimidad, la propiedad, la seguridad no han desaparecido, pero sí han cambiado de domicilio. Hoy habitan en servidores, nubes, dispositivos móviles y sistemas encriptados. Protegerlos con leyes de antaño es como poner cerrojos en casas que ya no existen. Panamá con las nuevas reformas intenta dar las herramientas necesarias para la persecución penal.

Miró Llinares (2012) refiere y subraya la necesidad de analizar y adaptar las respuestas legales a estos delitos, considerando las experiencias de otros países. Como algunos Estados Europeos y algunos de Latinoamérica como Colombia y México por mencionar solo algunos.

De acuerdo con De la Cruz (2006)

> La delincuencia organizada transnacional también comprende los fraudes bancarios, el uso masivo de tarjetas de crédito con identidades robadas, manipulaciones en la bolsa y en el mercado, en la información, el uso de altas tecnologías, la evasión tributaria, la falsificación de marcas, el fraude en perjuicio de instituciones financieras internacionales, el tráfico de obras de arte y la eliminación de desechos industriales tóxicos, entre otras. (pp. 49–50).

La lista resulta enorme en nuestra opinión, lavado de activos, lavado de dinero que cada vez prolifera más en nuestros Estados ante la mirada pasiva de quienes deben actuar contra este tipo de delitos y como no entenderlo, si los delincuentes actúan en el anonimato y cuando creemos conocerlos se nos escurren como agua en las manos, además cuentan con estructuras bien organizadas creando rutas delincuenciales, cuentan con personas muy preparadas, sumamente

astutas en el arte del engaño, ya sea usando ingeniería social, creando sociedades a nombre de testaferros, pagos con bitcoins, en fin, la realidad es que hacen ver que resulta fácil hacerse de recursos sin importar el daño que ocasionan a todos los seres humanos y a las economías de los Estados.

De acuerdo con Romeo Casabona y Rueda Martín (2023)

> Como nuestra organización social —la administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, la actividad de las empresas o de los particulares, la enseñanza y la investigación, etc.— ha pasado a depender de forma extraordinaria de unos sistemas y redes de información, los riesgos que se derivan de su vulnerabilidad han exigido garantizar una 'ciberseguridad' en el ciberespacio, es decir, en los sistemas de redes telemáticas, abiertas o cerradas. (p. 22).

Continúa diciendo; "Los costes de los «ciberataques» son evidentes y muy elevados ya que pueden poner en graves dificultades los servicios prestados por las Administraciones públicas, las infraestructuras críticas del Estado o las actividades de las empresas y ciudadanos". (p. 24).

El punto de vista de estos autores Casabona y Martin, no puede ser más certero, existen experiencias de extorsión a la administración de hospitales, bajo amenaza de hacer colapsar sus sistemas y hacer público el contenido hackeado de los datos de sus pacientes, exigiendo grandes cantidades de dinero a cambio de no molestarlos más, lo que orilla a invertir en ciberseguridad, bajo el concepto de contar con mayor seguridad implementan vigilancia tecnológica (sic).

En Panamá, la ciberseguridad ha dejado de ser un asunto para nerds paranoicos y se ha convertido en una cuestión de Estado.

Según TVN Noticias (2024), una organización promedio en el país ha sido blanco de 1,214 ataques cibernéticos en apenas seis meses. Una cifra que no requiere adjetivos se defiende sola. Y como era previsible, el sector bancario ese lugar donde se almacena datos sensibles y activos líquidos sigue siendo el favorito de los delincuentes digitales, tan voraces como invisibles.

En este caso Panamá ha tomado medidas como la reciente ley 478 de 4 de agosto de 2025 que introduce modificaciones cruciales al Código Penal, al Código Procesal Penal y a la Ley 11 de 2015. No es solo una actualización, es un intento por blindar el sistema jurídico frente a amenazas que ya no respetan ni geografías ni husos horarios.

El objetivo es claro, adaptarse a las exigencias del Convenio de Budapest, ese pacto internacional que, desde 2001, intenta imponer algo de orden en el caos digital global. Panamá ya dio el paso técnico; solo falta ratificarlo formalmente. En este caso hay motivos para celebrar. Porque el cibercrimen no tiene pasaporte, la cooperación jurídica internacional deja de ser solo un asunto diplomático para convertirse en una herramienta de supervivencia.

Ahora bien, la ley puede ser robusta, pero sin operadores capacitados es muy difícil su actuar. Aún queda el reto y no menor de fortalecer a quienes deben aplicarla, fiscales, jueces, policías, peritos informáticos... Un ejército aún en formación que necesita no solo recursos, sino también una comprensión profunda de que perseguir un cibercriminal requiere más que intuición jurídica, exige entender su lenguaje, su lógica y su camuflaje digital. Quizá lo inquietante no sea tanto la mutación del delito, sino nuestra resignación frente a ella.

Hemos aceptado que la seguridad penetre nuestra intimidad. Pero, ¿y si resulta que la vigilancia, como el crimen, también sabe adaptarse a cada época? En ese caso, el futuro no será ni de policías ni de ladrones, sino de observadores invisibles que deciden en silencio qué debemos temer y qué debemos callar.

Como señalan Arango Alzate, et.al, (2012), “la llamada vigilancia tecnológica (VT) no es un simple espía digital; es un sistema complejo que implica captar, analizar y difundir información de todo tipo —económica, política, tecnológica para anticipar riesgos y detectar oportunidades” (s.p)

Estos procesos de vigilancia a pesar que son de vieja data, se mantienen en el presente con modificaciones o adecuaciones acorde a la realidad social actual, consideramos que, si bien el comienzo fue pensando en competencia mercantil en apariencia, en el fondo ya existía un control no solo mercantil, también social y actualmente el manejo se relaciona con datos personales que por supuesto siempre estuvieron vinculados para poder impactar en el gusto de las personas y del mercado.

En realidad, hemos sido vigilados hace mucho, simple, al llegar a un aeropuerto en algunos cuentan con imágenes biométricas, así pueden identificar a una persona cuando interpol lanza la denominada alerta roja, en muchas ocasiones logran detener a un sujeto que cometió delito en lugar distinto de donde es detenido. Al ingresar a un residencial cuentan con video vigilancia y registran imágenes de todo el que accesa el portón de entrada, sean residentes o visitantes, sin contar con autorización alguna para ello, de tal manera que si una persona decide no dar sus datos personales simplemente no le dan acceso.

Según la Ley 81 de 2019, sobre protección de datos personales, el tratamiento de la información debe realizarse garantizando los derechos de seguridad, confidencialidad y consentimiento informado.

El contraste con el pasado hoy, las transacciones son invisibles, pero dejan un rastro mucho más visible, nuestros datos personales. Se supone que están “protegidos” por las instituciones financieras privadas y públicas, y toda empresa que tenga manejo digital, pero basta un clic imprudente o un servidor mal resguardado para que esa información se convierta en mercancía.

La vigilancia de esas transacciones digitales nació como un mecanismo de defensa. Sin embargo, en sus primeros pasos se parecía más a una voraz necesidad para la banca, datos recogidos sin consentimiento, utilizados con fines que poco tenían que ver con la seguridad del usuario. Solo la presión ciudadana y escándalos mediáticos obligaron a los reguladores a levantar la voz, aunque siempre como una reacción, y no como prevención.

El caso Cambridge Analytica es un ejemplo que no solo revela, sino que también inquieta: millones de usuarios entregaron voluntariamente sus datos en redes sociales, solo para descubrir después que habían alimentado uno de los experimentos de manipulación política más emblemáticos de nuestra era. Como advierte Véliz et al. (2023), “el debate contemporáneo no es técnico, es político. Y se centra en la disyuntiva entre libertad individual y control masivo, entre la promesa de conectividad y la realidad de la explotación de datos” (pp. 414-416).

El lado oscuro de todo esto son los denominados delitos cibernéticos, ransomware que paraliza hospitales enteros, fraudes electrónicos que pueden desaparecer ahorros de toda una vida, lavados digitales que hacen del dinero sucio un fantasma imposible de rastrear porque todo se hace desde el anonimato. Paradójicamente, la digitalización prometía democratizar las finanzas; en su lugar, abrió nuevas vías para la estafa y la corrupción.

La respuesta es concisa pero incómoda, lamentablemente las instituciones públicas o privadas se han visto en la necesidad de contratar servicios de vigilancia

tecnológica, lo ideal sería que estuviera muy bien regulada. Sin embargo, al mismo tiempo, necesitamos protegernos de la vigilancia tecnológica a pesar de todo. He aquí la paradoja esencial de nuestra era. La seguridad sin privacidad se convierte en un lugar en encierro; la privacidad sin seguridad, es un desafío digital. El desafío, quizá es el más complejo de nuestro tiempo, es encontrar ese equilibrio entre confianza y control.

La privacidad es un elemento importante de toda persona, en el pasado solo podíamos saber datos de personas, conversando con ellos, consultando un directorio, pero el Banco no facilitaba datos de ningún cliente bajo el argumento de confidencialidad y privacidad de información excepto cuando se requería por orden judicial.

En ese sentido Veliz (2023), indica “los datos personales deberían beneficiar a los ciudadanos, no deberían llenar los bolsillos de las corporaciones a expensas de los ciudadanos o la democracia” (p.426).

Veliz advierte, vivimos en la era de la información, pero apenas controlamos la información que entregamos. En teoría, deberíamos decidir qué datos compartir y cuáles resguardar; en la práctica, esa libertad se diluye entre datos confusos, además de políticas de privacidad que nadie ni los abogados más tenaces termina de entender.

El problema, dice Veliz, no es solo técnico, sino moral y económico. Los Estados y las empresas “lícitas” se enfrentan a una tentación difícil de resistir. Los datos personales son una moneda de cambio, y cada clic, cada compra o llamada, puede usarse digitalmente. No sorprende entonces que, sin saber cómo, un desconocido nos ofrezca por teléfono el “servicio ideal para nuestro perfil”. Uno se pregunta, con una mezcla de asombro y resignación, si ese perfil fue creado con permiso o simplemente tomado prestado.

Mientras más hablamos de privacidad, menos la tenemos. Cuanto más “conectados” estamos, más se diluyen los límites de lo íntimo. Tal vez el desafío real no sea tecnológico, sino ético, reaprender a decir “no” en un mundo que lo quiere saber todo de nosotros.

Zeballos Bethancourt (2023) Señala que “La protección de datos se refiere al conjunto de medidas destinadas a resguardar la información personal, garantizando que su uso o tratamiento por parte de instituciones públicas o privadas respete los derechos fundamentales de las personas, especialmente su intimidad, honor y vida familiar.” (p. 210).

Conclusiones

El recorrido realizado en esta investigación deja claro que los delitos financieros digitales avanzan a un ritmo que supera, por mucho, la capacidad de respuesta de los marcos legales actuales. La revisión de conceptos, datos recientes e informes internacionales confirma que estas conductas no solo son cada vez más frecuentes, sino también más refinadas y difíciles de rastrear. Todo esto coincide con lo planteado por autores como Miró Llinares o Díaz, que advierten desde hace años la transformación del delito en el entorno digital.

En el caso de Panamá, los resultados muestran que el país ha empezado a dar pasos importantes —como las reformas legales recientes y la intención de alinearse con el Convenio de Budapest—, pero todavía queda un camino largo. La falta de personal especializado, los vacíos de cooperación internacional y una estructura jurídica que aún responde con lógicas heredadas del siglo pasado dificultan una reacción efectiva frente a los delitos financieros digitales. Esta brecha entre lo que ocurre en el ciberespacio y lo que la ley puede abarcar se evidenció constantemente en los documentos revisados.

Otro punto que emergió con fuerza es la vigilancia tecnológica. Si bien las herramientas de monitoreo pueden ayudar a contener amenazas, su uso también

abre una serie de preguntas éticas que no se pueden ignorar. La posibilidad de que la seguridad termine convirtiéndose en un mecanismo de control excesivo está ahí, y los casos analizados lo demuestran. En sociedades que dependen cada vez más de sistemas digitales, la privacidad corre el riesgo de quedar relegada si no se establecen límites claros.

Por estas razones, la respuesta del Estado no puede limitarse únicamente a crear nuevas leyes. Además de actualizar la normativa, es indispensable invertir en capacitación técnica, fortalecer las instituciones encargadas de investigar estos delitos y establecer alianzas internacionales reales, no solo formales. Sin ese andamiaje, la legislación termina siendo insuficiente frente a delitos que no respetan fronteras ni horarios.

Finalmente, si algo queda claro después del análisis, es que la prevención sigue siendo la herramienta más sólida. La mayoría de los ataques digitales no solo explotan vulnerabilidades técnicas, sino también humanas. Una ciudadanía informada y con hábitos digitales seguros puede reducir considerablemente los riesgos.

En síntesis, las conclusiones permiten responder al objetivo del estudio: comprender el fenómeno del delito financiero digital desde su dimensión jurídica, identificar sus desafíos y proponer líneas de acción que permitan afrontarlo sin sacrificar derechos fundamentales en el proceso.

Referencias bibliográficas

Arango Alzate, B., Tamayo Giraldo, L., y Fadul Barbosa, A. (2012). Vigilancia tecnológica: metodologías y aplicaciones. Revista Electrónica Gestión de las Personas y Tecnología,5(13). https://www.redalyc.org/pdf/4778/477847114019.pdf

Bullock, J. B., Chen, Y.-C., Himmelreich, J., Hudson, V. M., Korinek, A., Young, M. M., y Zhang, B. (Eds.). (2023). The Oxford handbook of AI governance. Oxford University Press.

De la Cruz, O. (2006). Crimen organizado, delitos más frecuentes, Capítulo I, delincuencia organizada y globalización. Universidad Nacional Autónoma de México. https://archivos.juridicas.unam.mx/www/bjv/libros/5/2263/3.pdf

Díaz, R. M. (2021, septiembre). Estado de la ciberseguridad en la logística de América Latina y el Caribe (Serie Desarrollo Productivo No. 228; LC/TS.2021/108). Comisión Económica para América Latina y el Caribe (CEPAL). https://repositorio.cepal.org/handle/11362/47240

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill. https://esup.edu.pe/wpcontent/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20BaptistaMetodología%20Investigacion%20Cientifica%206ta%20ed.pdf

INCIBE-Ciberseguridad. (2024). Balance de ciberseguridad 2024: más de 97,000 incidentes gestionados.https://www.incibe.es/incibe/sala-de-prensa/incibe-presenta-su-balance-de-ciberseguridad-2024-con-mas-de-97000-incidentes

Ley 14 de mayo de 2007. (2007). Gaceta Oficial de Panamá. https://www.gacetaoficial.gob.pa/pdfTemp/25796/4580.pdf

Ley 18 de septiembre de 1982. (1982). Gaceta Oficial de Panamá. http://gacetas.procuraduria-admon.gob.pa/19667_1982.pdf

Ley 478 de agosto de 2025. (2025). Presidencia de la República de Panamá.https://www.presidencia.gob.pa/publicacion/presidente-mulino-sanciona-leyes-que-fortalecen-el-marco-legal-contra-la-ciberdelincuencia

Ley por la cual se aprueba el convenio sobre la ciberdelincuencia (Budapest, 23 de noviembre de 2001). (2013, octubre 22). Ministerio Público de Panamá. https://ministeriopublico.gob.pa/wp-content/uploads/2021/02/Ley-79-de-22-de-octubre-de-2013.pdf

Miró Llinares, F. (2018). Ciberdelincuencia y política criminal en la sociedad de la información. Marcial Pons, Ediciones Jurídicas y Sociales, S.A. https://www.infoem.org.mx/doc/biblioteca/accesoytrans/ciberdelitos/el-cibercrimen.pdf

Nava Garcés, A. (2017) Cibercriminalidad y redes sociales. (s.f.). Expediente INACIPE [Video]. YouTube. https://www.youtube.com/watch?v=eJIiziAUHhs&t=346s

Órgano Judicial. (2023). Encuesta sobre capacidades judiciales en ciberdelitos.https://www.organojudicial.gob.pa/uploads/blogs.dir/1/2024/06/456/anexo-situacion-ciberdelincuencia.pdf

Organización de las Naciones Unidas (ONU). (2022). Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). https://www.unodc.org/e4j/es/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

Panamá. (2019). Ley No. 81 de 2019, sobre protección de datos personales. Gaceta Oficial, N.º 28743-A, 29 de marzo de 2019.

Romeo Casabona, C. M., y Rueda Martín, M. Á. (2023). Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial. Volumen I: Ciberseguridad y ciberdelitos. Editorial Comares. https://www.comares.com/media/comares/files/toc149832.pdf

TVN Noticias. (2024, marzo 21). Ciberataques: ataques cibernéticos en Panamá, ¿cuál es su principal objetivo? Nacionales. https://www.tvn-2.com/nacionales/ciberataques-ciberneticos-expertos-advierten-organizacion-promedio-sufrio_1_2123000.html

Zeballos Bethancourt, S. C. (2023). La protección de datos personales en base a la Ley N.º 81 de 26 de marzo de 2019 “Sobre la protección de datos”. Anuario de Derecho, (52), 206–232. https://revistas.up.ac.pa/index.php/anuario_derecho/article/view/3451