

RECENSIÓN A VÍCTOR RAÚL ESPINOZA CALDERÓN: “LA PRUEBA DIGITAL EN EL PROCESO PENAL. ASPECTOS DOCTRINARIOS Y PROCESALES”

Junio de 2025, Lima (477 páginas)

Review of Víctor Raúl Espinoza Calderón: “La prueba digital en el proceso penal. Aspectos doctrinarios y procesales” (Digital evidence in criminal proceedings. Doctrinal and procedural aspects

FRANK CARLOS CABALLERO ZAVALA*

Recibido: 12.DIC.2025

Aprobado: 28.ENE.2026

RESUMEN: El autor presenta una resección del libro “La prueba digital en el proceso penal. Aspectos doctrinarios y procesales”, del año 2025, en la que se destacan los aspectos más relevantes de su estructura.

PALABRAS CLAVE: Prueba digital; redes sociales; resección; proceso penal; Víctor Raúl Espinoza Calderón.

ABSTRACT: The author presents a review of the 2025 book “*Digital Evidence in Criminal Proceedings: Doctrinal and Procedural Aspects*”, highlighting the most relevant features of its structure.

KEYWORDS: Digital evidence; social media; review, criminal procedure, Víctor Raúl Espinoza Calderón.

Este libro comienza en un escenario que nos resulta familiar, el mundo se ha ido mudando poco a poco a lo digital. Las conversaciones, las compras, las discusiones e incluso los conflictos han cruzado un umbral invisible para instalarse

* Abogado por la Universidad de Piura. Asistente de cátedra de Derecho Procesal Penal en la facultad de Derecho de la misma universidad. Coordinador académico del taller Litis Simulatio y cocoordinador del taller de Derecho Penal “José Gonzáles López” de la facultad de Derecho de la Universidad de Piura. Correo: frank.caballero.z@udep.edu.pe. Código ORCID: <https://orcid.org/0009-0004-0863-3977>.

en pantallas, servidores y redes. Pero, como suele ocurrir cuando la vida cambia de lugar, la justicia penal ha tenido que seguir ese rastro, a veces con dificultad, y preguntarse cómo investigar hechos que ya no dejan huellas en papel. En ese contexto de transición surge "La prueba digital en el proceso penal. Aspectos doctrinarios y procesales", cuyo propósito es ofrecer un panorama general acompañado de un análisis de doctrina y jurisprudencia para entender cómo la tecnología ha reconfigurado la prueba en el proceso penal.

Se trata de un libro de lectura accesible, aunque presupone que el lector ya ha transitado antes por los senderos del derecho procesal penal y de teoría de la prueba. No se trata de un manual clásico sobre la prueba en el sentido tradicional, ni de una simple descripción de los medios probatorios regulados en el Código Procesal Penal. Por el contrario, el lector encontrará aquí una propuesta orientada a comprender la prueba digital a partir de las transformaciones que han acompañado a la digitalización de la interacción social. El trabajo se compone de una nota introductoria, seis capítulos y una sección de tres apéndices dedicados a la jurisprudencia, la normativa y las directivas sobre prueba digital.

En el Cap. I. «Aspectos generales de la prueba», el autor hace una pausa necesaria. Antes de abordar cuestiones medulares, recuerda al lector algunos conceptos básicos sobre la prueba. Así, se explora qué es una fuente de prueba (p. 21), qué es un medio de prueba (p. 20), qué constituye el objeto probado (pp. 22-23) y los alcances de la libertad probatoria (p. 24). No lo hace para enseñar lo obvio, sino para advertir que todo lo que vendrá después solo puede entenderse si se tienen firmes estas nociones básicas.

En el Cap. II. «Derecho informático y su relación con la prueba digital», se traslada la discusión al terreno del derecho informático. En este apartado se abordan temas como la firma digital, la identidad electrónica, el comercio virtual, el notariado informático y la creciente virtualización del Estado, a la que se refiere como "gobierno digital" (p. 31). En este sentido, el autor muestra que Perú no es ajeno a la digitalización, sino que ha comenzado a adoptar medidas para armonizar los actos cotidianos con el entorno digital. De ahí su propuesta de revisar las distintas herramientas que ofrece el derecho informático. Esta exposición, lejos de constituir una mera presentación culturalmente enriquecedora, cobra pleno sentido en los capítulos siguientes, cuando se comprende la naturaleza de la prueba digital y su vínculo con la tecnología. No obstante, dado que esto ocurre recién en el capítulo tercero, es posible que el lector sienta la necesidad de volver a esta sección tras abordar el análisis específico de la prueba digital. También puede resultar llamativa la cuestión referida al documento, ya que si este se define como cualquier medio que permita soportar información (p. 36), ¿qué lo distingue realmente del documento electrónico? ¿Acaso la propia naturaleza del documento no abarca o subsume ya a los medios

tecnológicos como los videos o fotografías digitales? Parece ser así en la medida en que estos medios también albergan información. No obstante, en el siguiente capítulo se responde a esta pregunta y se explican las diferencias (p. 51).

En el Cap. III. «La prueba digital», se marca un punto de inflexión, ya que el autor decide responder a la pregunta ¿qué es la prueba digital? Para hacerlo, primero revisa qué se entiende por prueba (pp. 45-46) y cómo regula el Código Procesal Penal los medios de prueba típicos. Tras esto, llega a la conclusión de que ningún medio de prueba actual reconoce expresamente a la prueba digital (pp. 47-52). A continuación muestra que, pese a ello, la prueba digital existe, y la define como toda información en formato electrónico que solo puede comprenderse mediante un dispositivo electrónico (pp. 52-54). A partir de allí describe sus características, afirmando que toda prueba digital se caracteriza por ser volátil, alterable, duplicable y eliminable (pp. 57-58). Estos rasgos la vuelven poderosa, pero también peligrosa en manos equivocadas. Concluye señalando que su incorporación al proceso es válida siempre y cuando no se vulneren derechos fundamentales y se utilice el medio típico (reconocido legalmente) más análogo (p. 61).

El Cap. IV. «Tipos de contenidos digitales», lleva al lector al terreno más cotidiano y expone los distintos tipos de contenidos digitales utilizados hoy en día, como correos electrónicos, audios, fotografías, publicaciones en redes sociales. Esta presentación tiene la particularidad de que se hace desde un enfoque centrado en la prueba, es decir, el autor no se detiene únicamente a explicar en qué consiste el contenido (por ejemplo, qué es el correo electrónico), sino que aborda cómo incorporar estos contenidos al proceso penal. El autor también se encarga de advertir las problemáticas que enfrentan algunos contenidos digitales. Por ejemplo, analiza la manipulación de audios mediante inteligencia artificial, como es el caso de las voces simuladas, escenarios en lo que recomienda realizar cotejos y pericias especializadas para garantizar la autenticidad e integridad de los medios de prueba (pp. 74-75).

El Cap. V. «Redes sociales y prueba digital», se centra en las redes sociales, esos espacios donde hoy transcurre buena parte de la vida, y donde han comenzado a proliferar ilícitos al constituirse como una fuente de riesgos. El autor expone las dificultades que conlleva investigar hechos ilícitos cometidos en plataformas que carecen de regulación específica en el Perú (p. 136), que pueden afectar a derechos fundamentales en entornos como el metaverso (p. 134), o cuyos servidores se encuentran fuera del país, lo que dificulta la identificación de los presuntos responsables (pp. 137-139). También explica qué criterios debe usar el juez para valorar la prueba digital, tales como la autenticidad, la integridad, la valoración conjunta y la licitud (pp. 175-188). Finalmente, el autor recuerda que, si queremos recurrir a la prueba digital, no debemos olvidar que su tratamiento variará en función de la fase del proceso penal en la que nos encontremos (pp. 174-175). Así, la actividad proba-

toria no será la misma en la fase de ofrecimiento, admisión, actuación o valoración de la prueba.

En el Cap. VI. «Investigación tecnológica del delito y prueba digital», el autor presenta las técnicas de investigación tecnológica contempladas en el Código Procesal Penal, y explica que muchas de ellas surgieron de la necesidad específica de combatir la delincuencia organizada que opera en espacios digitales. Para perseguirla, el Estado debe seguirla por ese mismo camino, es decir, a través de mecanismos como la videovigilancia o los agentes encubiertos que permitan a los fiscales y efectivos policiales investigar el delito. No obstante, el autor también recuerda que quien mucho corre, pronto para, pues si bien con estas herramientas se busca asegurar la obtención de información para así determinar si la conducta incriminada es delictiva, actuar de cualquier forma puede conducir a errores y, en estos casos, a abusos. Por ello, aunque se han robustecido las facultades del órgano persecutor del delito, estas también encuentran límites, especialmente en escenarios en los que se tensionan la intimidad y la inviolabilidad de las comunicaciones (pp. 209-245).

El libro concluye dejando mucha tela que cortar, que sin duda convendría desarrollar en un estudio posterior específicamente dedicado a la parte especial. Para dicha tarea, se recuerda que el autor ya se ha ocupado de estudiar previamente un conjunto de delitos, en particular los delitos informáticos. Sin perjuicio de las implicaciones futuras que la obra pone sobre la mesa, Espinoza Calderón se encarga con éxito de evidenciar que la prueba digital si bien puede, de buenas a primeras, desafiar los parámetros tradicionales de la prueba (lo tangible), no le falta razón cuando recuerda que los principios probatorios clásicos (libertad de prueba) se mantienen inalterados frente a la prueba digital, siendo lo esencial que exista un medio de prueba reconocido por nuestra legislación que sea el más adecuado para utilizarla. Se trataría, en cierto modo, de proporcionarle un “ropaje” externo o formal que permita su incorporación al proceso penal. La cuestión, entonces, radica en determinar cuál de los medios de prueba existentes constituye el ropaje más idóneo para cada caso concreto. No obstante, aunque esta solución puede funcionar como una salida provisional, el verdadero problema surge cuando no exista un medio suficientemente análogo al que recurrir para introducir la prueba digital, ya sea por su propia complejidad técnica o por la naturaleza del soporte.

Las razones expuestas ponen de manifiesto que no se debe descartar la posibilidad de un eventual reconocimiento autónomo de la prueba digital. Esto cobra fuerza si se toma en cuenta que, a medida que avanza la tecnología nos encontraremos con nuevos escenarios delictivos menos convencionales que suscitarán el debate sobre la necesidad de dotar de autonomía a la prueba digital o si es suficiente recurrir a medios análogos como se viene haciendo actualmente. Aunque el autor no se dedica especialmente a ellos, se puede identificar que no solo se trata de fenómenos

ya conocidos como los *deepfakes* en delitos de pornografía o mensajes a través de redes sociales empleados para coordinar actos de corrupción pública, sino también de escenarios emergentes como el metaverso. En un entorno donde la interacción humana se desplazará hacia entornos virtuales, no debería causar sorpresa que los delitos podrían involucrar actos cometidos a través de avatares, transacciones con bienes digitales (NFTs), interacciones vocales y gestuales capturadas por sensores mediante dispositivos de realidad virtual (HaptX Gloves, Meta Quest 3), e incluso registros de conducta almacenados en servidores privados.

A mi parecer, este nuevo ecosistema tecnológico plantea interrogantes que pueden abordarse desde dos planos. El primero es el pragmático-procesal, centrado en cómo probar un hecho. Surgen así las siguientes preguntas: ¿cómo se puede acreditar que un avatar fue efectivamente controlado por el imputado en un caso de acoso sexual o actos de connotación sexual cometidos dentro del metaverso?, ¿cómo se puede demostrar que determinados actos de corrupción pública se llevaron a cabo mediante reuniones simuladas en espacios virtuales?, ¿es suficiente la cadena de custodia tradicional cuando la prueba no se halla en un dispositivo físico, sino en una plataforma transnacional cuyos servidores contienen registros clave? En un segundo plano, el político-criminal, la discusión gira en torno a los actos de gobierno dirigidos a la prevención de problemas sociales de criminalidad. La cuestión radica en que la construcción e implementación de políticas públicas no debe desatender principios esenciales como la dignidad, legalidad y seguridad en la vida social. De lo contrario, las medidas adoptadas para prevenir y combatir el delito podrían derivar en mecanismos de vigilancia desproporcionados que recuerdan a la novela “1984” de George Orwell, donde el control absoluto de las comunicaciones (a cargo de la policía del pensamiento) deja escaso o nulo margen para la privacidad y la intimidad.

En mi opinión, uno de los aportes más logrados del trabajo (y de gran interés para los operadores de justicia) es la claridad con la que Calderón Espinoza aborda los criterios de valoración de la prueba digital. Su análisis del principio de autenticidad (correspondencia entre lo presentado y el dispositivo original que lo contiene) resulta especialmente útil en los delitos contra la administración pública, ya que un correo electrónico o *screenshots* de las conversaciones de WhatsApp pueden servir como indicios (aunque no se agotan ahí) para construir una hipótesis de un acuerdo colusorio o sobornos. En ese orden, este principio recuerda que no debe pasarse por alto que hoy en día es preocupantemente fácil alterar los correos electrónicos, ya sea mediante edición, suplantación del remitente o manipulación del asunto. En este sentido, para acreditar una conversación que tuvo lugar en un entorno digital, no basta con imprimir el mensaje, sino que hay que verificar el archivo nativo y sus metadatos. Lo mismo ocurre con las capturas de pantalla, ya que, por su propia naturaleza son representaciones físicas y no el dato original, lo que permite que su



manipulación pueda pasar inadvertida mediante inteligencia artificial (como Pixel-cut) si antes no se contrasta la información con el dispositivo que la contiene.

En suma, el trabajo de Espinoza Calderón merece ser destacado porque no solo articula el diálogo entre el derecho procesal penal, la tecnología y la teoría de la prueba, sino porque enfrenta de manera sistemática los múltiples desafíos que plantea la prueba digital en el proceso penal. Siendo este el panorama, la contribución del autor resulta valiosa porque ofrece criterios y reflexiones que permiten afrontar un ecosistema probatorio en constante transformación, sin renunciar a los fines del proceso penal (la verdad, la justicia y la paz jurídica) y a las garantías que caracterizan a nuestro sistema penal acusatorio formal.