



Revista Iberoamericana de Derecho, Cultura y Ambiente



Edición Nº 9 – Julio de 2026

Capítulo de Derecho Penal y Criminología

www.aidca.org/revista

**VIDENCIA DIGITAL Y SU VALIDEZ PROBATORIA EN EL PROCESO JUDICIAL
DESAFÍOS JURÍDICOS, GARANTÍAS CONSTITUCIONALES Y VALORACIÓN
DE LA PRUEBA TECNOLÓGICA**

Por el Dr. Ángel Nassif¹

Introducción

La revolución tecnológica ha modificado profundamente la dinámica social, económica y jurídica contemporánea. Gran parte de las relaciones humanas, comerciales e institucionales se desarrollan actualmente mediante plataformas digitales, dispositivos electrónicos y sistemas informáticos que generan, almacenan y transmiten información de manera permanente. En consecuencia, los conflictos sometidos a conocimiento judicial contienen cada vez con mayor

¹ Dr. Ángel Nassif & Asociados Catamarca 250 – 4200 Santiago del Estero Francisco Solano 373 Of 2 Altos
– 4220 Termas de Río Hondo Telef: 3856986571 Responder Reen



frecuencia elementos tecnológicos susceptibles de ser utilizados como medios probatorios.

La llamada “evidencia digital” se ha convertido así en uno de los instrumentos más relevantes dentro del moderno derecho probatorio. Mensajes de WhatsApp, correos electrónicos, registros de geolocalización, publicaciones en redes sociales, archivos multimedia, documentos electrónicos y metadatos integran hoy el universo cotidiano de la litigación judicial.

Sin embargo, la incorporación de este tipo de prueba plantea importantes desafíos jurídicos. La facilidad de reproducción, alteración o manipulación de los datos digitales exige nuevas pautas de autenticación, conservación y valoración. A diferencia de la prueba documental clásica, la evidencia digital posee características técnicas propias que obligan a los operadores jurídicos a compatibilizar principios tradicionales del derecho procesal con herramientas provenientes de la informática forense.

El problema central no radica únicamente en determinar si la evidencia digital puede ser admitida como prueba, sino principalmente en establecer bajo qué condiciones adquiere eficacia probatoria suficiente para generar convicción judicial sin afectar garantías constitucionales fundamentales como la intimidad, la privacidad, el secreto de las comunicaciones y el debido proceso legal.

En este contexto, la doctrina y la jurisprudencia han debido construir progresivamente criterios orientados a determinar la validez y eficacia de la prueba digital, reconociendo que la verdad procesal contemporánea ya no puede desvincularse del entorno tecnológico en el cual se producen los hechos litigiosos.

El presente trabajo tiene por objeto analizar la naturaleza jurídica de la evidencia digital, sus formas de obtención, los requisitos de autenticidad e integridad, la problemática de la cadena de custodia, y especialmente su valor probatorio dentro del proceso judicial argentino.

I. Concepto y naturaleza jurídica de la evidencia digital



La evidencia digital puede definirse como toda información o dato de valor probatorio almacenado, transmitido o generado mediante dispositivos electrónicos o sistemas informáticos.

Comprende: documentos electrónicos, mensajes de mensajería instantánea, correos electrónicos, registros informáticos, archivos multimedia, metadatos, bases de datos, registros de navegación, información almacenada en servidores o sistemas en la nube.

Su naturaleza jurídica ha sido objeto de debate doctrinario. Algunos autores la consideran una variante moderna de la prueba documental, mientras que otros sostienen que constituye una categoría autónoma debido a sus particularidades técnicas.

Lo cierto es que la evidencia digital presenta características distintivas:

1. Intangibilidad

La información digital carece de soporte físico perceptible de manera inmediata. Los datos existen como secuencias electrónicas interpretables únicamente mediante sistemas tecnológicos.

2. Volatilidad

Puede modificarse, eliminarse o transferirse con extrema facilidad y rapidez.

3. Replicabilidad

La información puede copiarse infinitamente sin pérdida aparente de calidad.

4. Dependencia tecnológica

Su acceso e interpretación requieren dispositivos, software y conocimientos técnicos específicos.

Estas características explican la necesidad de establecer procedimientos especiales para garantizar su autenticidad y eficacia procesal.

II. Obtención de la evidencia digital y garantías constitucionales

La validez de la evidencia digital depende, en primer lugar, de la legalidad de su obtención.



La Constitución Nacional protege expresamente: la privacidad, la intimidad, el secreto de las comunicaciones, el debido proceso legal.

En consecuencia, la obtención de evidencia digital mediante mecanismos ilegítimos puede generar nulidad probatoria.

1. Obtención lícita

La evidencia digital puede obtenerse legítimamente mediante: consentimiento del titular del dispositivo, secuestro judicial autorizado, allanamientos, requerimientos judiciales a empresas tecnológicas, entrega voluntaria de archivos, pericias informáticas autorizadas.

La intervención judicial resulta particularmente necesaria cuando se pretende acceder a: teléfonos celulares, cuentas privadas, correos electrónicos, sistemas protegidos por claves, comunicaciones reservadas.

2. Prueba ilícita

La obtención clandestina o ilegítima de datos digitales puede vulnerar garantías constitucionales.

Resultan inadmisibles, por ejemplo: hackeos, acceso no autorizado a cuentas, interceptación ilegal de comunicaciones, utilización de software espía, extracción irregular de datos privados.

La doctrina de la “fruta del árbol venenoso”, receptada jurisprudencialmente, impide otorgar eficacia a la prueba obtenida con violación de derechos fundamentales.

La Corte Suprema de Justicia de la Nación ha sostenido reiteradamente que el proceso judicial no puede legitimar actuaciones estatales o particulares violatorias de garantías constitucionales.¹

III. Preservación de la evidencia digital y cadena de custodia

Uno de los aspectos más sensibles de la prueba digital es su preservación.

La facilidad de alteración de los archivos obliga a adoptar mecanismos técnicos destinados a garantizar: autenticidad, integridad, trazabilidad.

1. Cadena de custodia



La cadena de custodia constituye el conjunto de procedimientos destinados a documentar:

quién obtuvo la evidencia, cuándo, cómo fue almacenada, quién tuvo acceso a ella, qué manipulaciones se realizaron.

La ausencia de cadena de custodia adecuada puede debilitar significativamente la fuerza probatoria de la evidencia digital.

2. Copia forense

En informática forense se utiliza frecuentemente la llamada “imagen espejo” o copia bit a bit del dispositivo original.

Este procedimiento permite trabajar sobre una copia exacta evitando alterar el soporte original.

Asimismo, se utilizan códigos hash (MD5, SHA) que funcionan como “huellas digitales” del archivo, permitiendo verificar que no sufrió modificaciones posteriores.

IV. Valor probatorio de la evidencia digital

La evidencia digital no posee valor probatorio automático. Su eficacia depende de la valoración judicial conforme las reglas de la sana crítica racional.

1. Autenticidad

El juez debe determinar si el archivo proviene efectivamente de quien se afirma.

La autenticidad puede acreditarse mediante: pericia informática, reconocimiento de parte, metadatos, registros técnicos, corroboración contextual.

2. Integridad

Debe verificarse que la información no haya sido modificada.

La utilización de herramientas forenses y códigos hash constituye actualmente uno de los mecanismos más eficaces para garantizar integridad.

3. Corroboración



La jurisprudencia suele exigir que la evidencia digital sea analizada conjuntamente con otros elementos probatorios.

Por ejemplo: testimonios, informes periciales, documentación complementaria, registros telefónicos.

4. Capturas de pantalla

Uno de los problemas más frecuentes se vincula con las simples capturas de pantalla.

Las mismas poseen valor indiciario limitado cuando no se encuentran respaldadas por: archivos originales,

constatación notarial, pericia informática, reconocimiento de autenticidad.

Debido a la facilidad de edición digital, los tribunales suelen exigir corroboración adicional.

V. Jurisprudencia sobre evidencia digital

La jurisprudencia argentina ha evolucionado significativamente en materia de prueba digital.

La Corte Suprema y tribunales inferiores han admitido progresivamente correos electrónicos mensajes de texto, conversaciones de WhatsApp, publicaciones en redes sociales, registros electrónicos.

Sin embargo, la admisión suele condicionarse a la acreditación de autenticidad e integridad.

En numerosos precedentes se ha señalado que la prueba digital debe ser analizada con criterio prudente, atendiendo especialmente a la posibilidad técnica de manipulación.

Asimismo, diversos tribunales han reconocido valor probatorio a conversaciones de WhatsApp cuando fueron acompañadas de pericia informática o reconocimiento de las partes.

VI. La importancia de la pericia informática

La informática forense ocupa hoy un rol central en la litigación moderna.



El perito informático permite: verificar autenticidad, analizar metadatos, recuperar archivos eliminados, determinar alteraciones, reconstruir actividad digital.

En muchos casos, la eficacia de la prueba depende directamente de la calidad técnica de la pericia realizada.

Por ello, el abogado litigante contemporáneo debe comprender que la evidencia digital exige una interacción permanente entre derecho y tecnología.

VII. Desafíos actuales

La expansión de nuevas tecnologías genera desafíos crecientes: inteligencia artificial, deep fakes,

manipulación audiovisual, criptografía, almacenamiento en la nube, anonimización digital.

Estas herramientas incrementan las dificultades de autenticación y obligan a replantear permanentemente los estándares probatorios tradicionales.

El derecho procesal enfrenta así el desafío de mantener equilibrio entre: innovación tecnológica, eficacia investigativa, protección de derechos fundamentales.

Conclusión

La evidencia digital constituye actualmente uno de los pilares fundamentales del moderno sistema probatorio.

La creciente digitalización de las relaciones humanas ha transformado profundamente la actividad judicial, imponiendo nuevas exigencias técnicas y jurídicas tanto a magistrados como a abogados litigantes.

Sin embargo, la eficacia de la prueba digital no depende únicamente de su contenido, sino fundamentalmente de la forma en que fue obtenida, preservada y presentada en el proceso.

La autenticidad, integridad, legalidad y trazabilidad constituyen requisitos esenciales para otorgarle validez probatoria.



En este contexto, la informática forense adquiere un rol decisivo, permitiendo dotar de confiabilidad técnica a los datos electrónicos incorporados al expediente judicial.

El proceso judicial contemporáneo exige entonces una nueva mirada interdisciplinaria, donde derecho y tecnología interactúan permanentemente en la búsqueda de la verdad material sin sacrificar garantías constitucionales fundamentales.

La evidencia digital ya no representa el futuro de la litigación: constituye definitivamente su presente.

Bibliografía

PALAZZI, Pablo Andrés, Delitos Informáticos, Abeledo Perrot, Buenos Aires.

DEVIS ECHANDÍA, Hernando, Teoría General de la Prueba Judicial, Temis.

ARAZI, Roland, La Prueba en el Proceso Civil, Rubinzal Culzoni.

CARNELUTTI, Francesco, La Prueba Civil.

FALCÓN, Enrique M., Tratado de la Prueba, Astrea.

PALACIO, Lino Enrique, Derecho Procesal Civil.

Pablo A. Palazzi — Los delitos informáticos en el Código Penal Editorial Abeledo Perrot