LA NULIDAD PROCESAL POR RUPTURA DE LA CADENA DE CUSTODIA DIGITAL: ESTÁNDARES COMPARADOS EN LA JURISPRUDENCIA ARGENTINA Y ESPAÑOLA[1]

Wendy Requejo Passoni[2]

1. INTRODUCCIÓN

En los últimos años, la intervención de las fuerzas policiales y de inteligencia en el ciberespacio ha llamado la atención de los mecanismos de supervisión del control social más formalizado, precisamente porque, en ocasiones, dichas intervenciones vulneran derechos y garantías. Así lo evidencia EUROPOL (2025), al afirmar que la transformación del panorama tecnológico dificulta mantener los actos de investigación policial sigan bajo control estatal (p. 23).

Efectivamente, no son pocos los casos en los que las actuaciones de los agentes policiales encargados de llevar adelante investigaciones enfrentan desafíos vinculados con el conocimiento técnico y los límites legales que rigen su accionar. En numerosas ocasiones, el desconocimiento de dichos límites constituye una práctica recurrente que, lamentablemente, incide de manera directa en elementos probatorios esenciales para el desarrollo y la validez de los procesos judiciales.

2. NULIDAD DE LA PERICIA DIGITAL Y RUPTURA DE LA CADENA DE CUSTODIA

Este estudio se centra en el análisis de la causa "Fiscal s/ apela declaración de nulidad de informe pericial"[3], resuelta el 24 de mayo de 2012, mediante la cual un tribunal de apelaciones se pronuncia respecto de la impugnación presentada contra una decisión de primera instancia. El tribunal decidió "decretar la nulidad en la presente causa N° 12446/08 y respecto de la pericia practicada por la División Apoyo Tecnológico de la Policía Federal Argentina sobre las computadoras secuestradas en los domicilios ambas de esta Ciudad; como también así de todo acto que hubiere tenido lugar en la causa en su consecuencia: particularmente la pericia encomendada a los técnicos de la

[1] Cítese como Requejo Passoni, W. 2025. La nulidad procesal por ruptura de la cadena de custodia digital: estándares comparados en la jurisprudencia argentina y española, *Estudios sobre jurisprudencia*, 326-345.

[2] Licenciada en Derecho por la Universidad San Martín de Porres (Perú), con dos másteres en Derecho Penal (Universidad de Salamanca, España) y en Derecho de la Ciberseguridad y Entornos Digitales (Universidad de León, España). Actualmente cursa estudios en el Programa de Doctorado "Estado de Derecho y Gobernanza Global" en la Universidad de Salamanca, es Investigadora en formación en el Centro de Investigación para la Gobernanza Global (CIGG) de la misma universidad. Correo de contacto: wrequejopassoni@usal.es ORCID: https://orcid.org/0000-0001-9952-2199.

[3] Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, Sala I, "Fiscal s/apela declaración de nulidad de informe pericial (Causa N° 46744)", rta. 24/05/20212. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5275 [último ingreso 01/10/2025].

Universidad de Buenos Aires, sus conclusiones, la información obtenida y la extracción de *test*imonios ordenadas al respecto".

El contexto fáctico se enmarca en un proceso penal seguido contra un exfuncionario del Ministerio de Transporte de la Nación, en el cual se llevaron a cabo diligencias investigativas que incluyeron el secuestro de computadoras halladas en su domicilio, en el marco de una investigación por presunto enriquecimiento ilícito. El análisis de dichos dispositivos y de la información recolectada dio lugar a un debate sobre el accionar de las fuerzas policiales a cargo de la investigación con evidencia digital.

En un primer momento, la División Apoyo Tecnológico de la Policía Federal Argentina (PFA) llevó a cabo un peritaje inmediato tras el secuestro de los dispositivos. Sin embargo, este procedimiento generó suspicacias, dado que no se notificó oportunamente a la defensa, lo cual motivó objeciones en cuanto a la posible contaminación de la evidencia. Esta omisión fue considerada violatoria a la obligación de notificar a la defensa en caso de medidas irreproducibles. Si bien la Fiscalía había sido debidamente informada, el Tribunal descartó el argumento de urgencia o simplicidad alegada por la PFA, subrayando la complejidad técnica inherente a este tipo de diligencias periciales.

Asimismo, se cuestionó que durante la pericia inicial no se hubiera utilizado bloqueadores de escritura, para evitar la introducción de datos contaminantes. Tampoco se documentaron adecuadamente las herramientas empleadas, las fechas de intervención ni las operaciones técnicas realizadas, lo que comprometió aún más la validez del procedimiento.

Posteriormente, se ordenó una segunda pericia, esta vez a cargo de expertos de la Universidad de Buenos Aires, con el propósito de garantizar la imparcialidad en el análisis. No obstante, los peritos concluyeron que la ausencia de documentación respaldatoria y la falta de medidas básicas de resguardo, tales como la desactivación de puertos eléctricos, comprometían la integridad de la evidencia. En esta instancia se advirtió que las falencias del primer peritaje podrían haber afectado el estado original material, lo que imposibilitaba asegurar la fidelidad de los datos. Para paliar estos efectos, los técnicos de la UBA emplearon bloqueadores de escritura; sin embargo, la duda respecto de la integridad de la evidencia ya se encontraba instalada en el proceso.

Frente a las irregularidades acumuladas, se dispuso un tercer análisis pericial, esta vez a cargo de especialistas de la Universidad Tecnológica Nacional (UTN). Este nuevo peritaje no solo buscaba acceder a la información contenida en los dispositivos, sino también verificar si su integridad se mantenía intacta, es decir, si no había existido alteración alguna en el contenido. Las conclusiones de este informe fueron categóricas: no era posible asegurar que el contenido examinado por la UBA coincidiera con el que existía al momento del secuestro. Se detectaron numerosos archivos creados o modificados

durante el período en que el material estuvo bajo custodia policial, varios de ellos vinculados con hechos relevantes para la causa. Incluso se identificaron archivos cuya fecha de modificación era anterior a la de creación, lo que constituye una inconsistencia técnica grave. Este mismo punto fue retomado durante la declaración de un perito ingeniero convocado por la Fiscalía, quien reconoció que se habría producido una ruptura en la cadena de custodia durante la intervención de la PFA, atribuyéndola a una negligencia operativa.

Como consecuencia de todas estas irregularidades, el Tribunal consideró que las evidencias digitales se encontraban contaminadas, eran irreproducibles y, por ende, carecían de fiabilidad probatoria. En virtud de ello, se decretó la nulidad tanto del peritaje realizado por la PFA como del posterior llevado a cabo por la UBA. No obstante, la investigación por enriquecimiento ilícito continuó sobre la base de otras pruebas válidamente incorporadas al expediente.

Finalmente, en el año 2024, la Sala III de la Cámara Federal de Casación Penal, integrada por los jueces Mariano Borinsky, Daniel Petrone y Alejandro Slokar, confirmó las condenas impuestas por el Tribunal Oral en lo Criminal Federal N° 6 de la Capital Federal al exfuncionario de Transporte, en el marco del juicio por hechos de enriquecimiento ilícito y corrupción cometidos entre 2003 y 2010. Dado el perfil público del acusado, el caso tuvo una gran repercusión mediática y presenta múltiples aristas de análisis. Sin embargo, en este trabajo nos limitaremos a examinar únicamente uno de sus aspectos: la cadena de custodia de la evidencia digital.

3. DEBATES JURISPRUDENCIALES RELEVANTES PARA EL OBJETO DE ESTUDIO

La causa N° 46.744 constituye un antecedente paradigmático en la jurisprudencia nacional respecto de la nulidad probatoria derivada de la ruptura en la cadena de custodia de evidencias digitales. Su relevancia no solo radica en el carácter mediático del proceso, sino también en el pronunciamiento judicial sobre los requisitos mínimos que deben observarse para garantizar la integridad de la prueba digital.

Una de las controversias centrales en la resolución judicial del 24 de mayo de 2012 fue la valoración del accionar de la División Apoyo Tecnológico de la Policía Federal Argentina (PFA), cuya intervención fue cuestionada desde distintas aristas. Frente a los planteos de nulidad interpuestos por la defensa, la Fiscalía sostuvo una postura opuesta: argumentó que se trataba de una diligencia sencilla y no compleja, y que no era exigible la notificación previa a las partes. No obstante, el tribunal de apelaciones desestimó esta posición al considerar que la urgencia alegada no estaba debidamente fundamentada, y que, en efecto, la omisión de notificación a la defensa —pese a haberse informado al Fiscal— vulneraba expresamente los derechos garantizados en los artículos 200, 201 y 258 del Código Procesal Penal de la Nación.

Tal como se expone en la resolución judicial bajo análisis, "la mera trascripción de esa palabra [urgencia] no puede suplantar la indicación de los motivos en los que ella se debe asentar, pues está en juego un derecho que la ley acuerda a las defensas bajo expresa sanción de nulidad". Esta afirmación cobra especial relevancia si se considera que, pocos días después del primer peritaje —realizado sin intervención de las partes—, se ordenó una segunda pericia sobre los mismos dispositivos, esta vez con la presencia de la defensa. En este sentido, el tribunal concluyó que el apuro evidenciado inicialmente no tenía como fin prioritario la evaluación del contenido probatorio de los archivos secuestrados, sino que respondió a una *mala praxis* de las fuerzas policiales que terminó por debilitar gravemente la fiabilidad de la prueba.

La jurisprudencia nacional ha reforzado esta línea interpretativa en otros precedentes de características similares. En el marco de la causa N° 14.545/2010[4], relativa al incidente de nulidad promovido por las defensas de dos imputados, la Sala V de la Cámara Nacional de Apelaciones en lo Criminal y Correccional adoptó un enfoque restrictivo respecto del valor probatorio de evidencia digital obtenida con defectos procedimentales. En dicha oportunidad, el tribunal consideró acreditada la existencia de serias irregularidades durante el procedimiento de secuestro, copiado y conservación del material informático, entre ellas: la ausencia de notificación a la defensa, la informalidad en el registro de operaciones técnicas y la omisión de medidas básicas de resguardo que garantizaran la inalterabilidad de los datos. En consecuencia, se resolvió hacer lugar al pedido de nulidad, declarando inválidas las actas y todas aquellas labradas en su consecuencia. Esta decisión reafirmó que las garantías procesales no pueden quedar supeditadas al argumento de eficiencia investigativa, mucho menos en contextos donde lo que está en discusión es el ejercicio de derechos fundamentales vinculados a la privacidad, el debido proceso y la defensa en juicio.

Este desarrollo jurisprudencial abre, sin embargo, una serie de interrogantes doctrinales que ameritan nuestra atención ¿Debe considerarse que toda afectación a la cadena de custodia en materia digital conlleva necesariamente una nulidad insanable? ¿O podría ponderarse, caso por caso, el grado de afectación efectiva sobre los derechos involucrados?

En efecto, el conflicto no se reduce únicamente al derecho al debido proceso, sino que también puede ser examinado a la luz del desarrollo de nuevas doctrinas jurídicas, como la teoría de los derechos digitales. Dentro de esta perspectiva, derechos como la protección de datos personales, la autodeterminación informativa y el derecho a no ser objeto de decisiones automatizadas sin supervisión humana, exigen una revisión crítica

[4] Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala V, "Colli, Matías Gabriel – Incidente de nulidad (Causa N° 14.545/2010, Exp. J119)", rta. 11/09/2015. Disponible en https://d26lpennugtm8s.cloudfront.net/stores/910/619/rte/OLX%20v%20Colli%20(cadena%20de%20custodia%20%20proc%20penal)%20(1).pdf [último acceso 01/10/2025].

de las prácticas tradicionales de investigación penal, en especial aquellas relacionadas con el acceso, almacenamiento y análisis de datos electrónicos.

Desde esta óptica, resulta imprescindible advertir que la cadena de custodia no se limita a prevenir modificaciones en los archivos, sino que abarca además el contexto técnico de su adquisición, la trazabilidad de cada intervención y la transparencia en los procedimientos. En este sentido, una ruptura o manejo defectuoso de la cadena de custodia puede entrar en tensión directa con estos derechos emergentes, afectando no solo la validez de la prueba, sino también el respeto a principios fundamentales en el entorno digital.

Por otra parte, desde un enfoque procesal, se plantea el debate en torno a la carga de la prueba: ¿sobre quién recae la obligación de acreditar la conservación de la cadena de custodia? Si bien buena parte de la doctrina coincide en atribuir que es el órgano acusador quien debe garantizar la licitud e integridad del material probatorio, esta presunción adquiere particular complejidad en el ámbito de la evidencia digital. En este terreno, la sofisticación tecnológica de los dispositivos y la multiplicidad de vectores posibles de alteración —involuntaria o maliciosa— imponen una carga de diligencia técnica reforzada. Por ello, no bastaría con la afirmación genérica de que la prueba fue resguardada conforme a derecho: resultaría imprescindible documentar, de manera precisa y verificable, cada etapa del procedimiento técnico, desde la adquisición de los datos hasta su análisis pericial.

Finalmente, en el caso bajo estudio, tratándose del secuestro de computadoras —aunque, en rigor, la información relevante se encuentra almacenada en los discos duros, que son los dispositivos físicos propiamente dichos—, resulta necesario reflexionar sobre si el uso exclusivo de herramientas como el código *hash* es una garantía suficiente de integridad. Si bien el *hash* constituye una herramienta fundamental para verificar la integridad binaria de los datos, su eficacia probatoria depende de que haya sido generado en condiciones estrictamente controladas, debidamente documentadas y técnicamente auditables. No obstante, en ciertas ocasiones, se han advertido prácticas que implican la alteración del contenido digital mediante técnicas como el borrado magnético, especialmente en el caso de discos duros tradicionales. Este tipo de intervenciones, generalmente motivadas en alterar o hacer inaccesible la información, compromete de forma directa la autenticidad del soporte físico que contiene la información. En tales circunstancias, el código *hash*, lejos de ofrecer una garantía concluyente, resultaría insuficiente para asegurar la inalterabilidad del contenido, afectando gravemente su aptitud como medio de prueba válido dentro del proceso penal.

4. MIRADA COMPARATIVA DE LA JURISPRUDENCIA ARGENTINA Y ESPAÑOLA

4.1 Jurisprudencia argentina sobre la cadena de custodia digital

En Argentina, la afectación de la cadena de custodia en materia digital no genera, de forma automática, una nulidad insanable. Por el contrario, la línea jurisprudencial ha evolucionado hacia una ponderación caso por caso, basada en el principio de razonabilidad, en la existencia de un perjuicio concreto para el imputado y en la necesidad de preservar derechos fundamentales en el entorno digital, sin desconocer la singular naturaleza de esta clase de evidencia.

En el precedente "VC, E s/ recurso de casación"[5], la Sala I de la Cámara Federal de Casación Penal (CFCP) reconoció la trascendencia del respeto a la cadena de custodia en evidencia digital, afirmando que su mantenimiento resulta "ineludible" para garantizar su "credibilidad, legitimidad, identidad, integridad y pureza". No obstante, dejó en claro que la omisión de prácticas técnicas recomendadas –como la generación de códigos *hash* o el uso de bloqueadores de escritura– no conlleva por sí sola la invalidez de la prueba, si no se demuestra un perjuicio concreto para el imputado. En esa línea, se sostuvo que, en contextos de urgencia, como durante la contención de un ataque informático, puede existir un margen razonable de actuación por fuera de los protocolos, siempre que los mecanismos adoptados resulten idóneos y puedan ser respaldados con otras pruebas (por ejemplo, *test*imonios o informes posteriores).

Este criterio de flexibilidad evaluativa fue ratificado en la causa "H, Y E s/ recurso de casación"[6], por la Sala II de la CFCP, donde se rechazó la nulidad pretendida por la defensa pese a que el dispositivo secuestrado había sufrido un daño mientras estaba bajo custodia. El tribunal ponderó que el juzgador basó su decisión en múltiples elementos probatorios válidamente incorporados y que la defensa tuvo oportunidad suficiente de ejercer sus facultades, por lo que no se verificó una lesión al derecho de defensa.

La misma Sala, en la causa "B, C.A. y otros s/ recurso de casación"[7], validó prácticas de resguardo digital realizadas por personal informático durante un allanamiento, aun cuando no se había producido una "desintervención" formal de los dispositivos. El fallo rechazó la nulidad argumentando que no se extrajo información de los dispositivos, y que el procedimiento se ajustó a lo dispuesto en los artículos 231, 233 y 261 del CPPN. Asimismo, subrayó que la falta de desintervención no es un requisito legal, y que la validez de la evidencia depende de su trazabilidad, no de ritualidades.

[5] Cámara Federal de Casación Penal, Sala I. Sala I, FRO 19631/2017/TO1/5/CFC2 "VC, E s/ recurso de casación", reg. 1434/23, rta. 28/11/2023. Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].
[6] Cámara Federal de Casación Penal, Sala II. FCT 1511/2018/TO1/20/CFC7 "H, Y E s/ recurso de casación", reg. 919/22, rta. 12/7/2022. Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].
[7] Cámara Federal de Casación Penal, Sala II. FMZ 43540/2017/TO1/66/CFC4 "B, CA y otros s/ recurso de casación", reg. 867/24, rta. 6/8/2024. Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].

En sentido análogo, en la causa "Incidente N° 93 -Querellante: FK., CE y otros imputado: M, F y otros s/incidente de nulidad"[8], la Sala IV de la CFCP concluyó que el planteo de nulidad sobre la cadena de custodia del contenido de un teléfono celular no constituía cuestión federal revisable, porque no se había demostrado un perjuicio concreto y la defensa se había limitado a invocar formalismos sin mostrar afectación real al derecho de defensa.

La jurisprudencia reciente también ha puesto énfasis en el control de los actos posteriores y la posibilidad de ratificación técnica. Así, en la causa "M, L.D. y otros s/ recurso de casación"[9], la Sala II de la CFCP sostuvo que la evidencia digital era válida porque las actas de procedimiento, registros fotográficos, coincidencias de IMEI y *hash* de extracción confirmaban la identidad de los teléfonos peritados, desvirtuando las meras conjeturas de la defensa.

Por contraposición, en la causa "Fiscal s/apela declaración de nulidad de informe pericial", la Sala I de la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, decretó la nulidad de la evidencia digital porque se verificaron múltiples irregularidades acumulativas: ausencia de notificación a la defensa, falta de documentación técnica, inexistencia de bloqueadores de escritura y generación de archivos durante la custodia policial. Las conclusiones de la Universidad Tecnológica Nacional confirmaron que no era posible garantizar la integridad del contenido examinado, motivo por el cual el tribunal concluyó que la cadena de custodia estaba irremediablemente rota y la prueba contaminada.

De este contraste surge que la nulidad por violación a la cadena de custodia digital no es automática ni dogmática, sino que requiere demostrar un perjuicio real, irreparable y verificable. En la causa "S, C.G. s/ recurso de casación"[10] se ilustra esta postura al validar registros de audio y video obtenidos de manera informal, en un contexto carcelario, ponderando la gravedad institucional de los hechos y la multiplicidad de otras pruebas coincidentes. Similar criterio se adoptó en la causa "Y, D.E. y otros s/ recurso de

[8] Cámara Federal de Casación Penal, Sala IV. FLP 14149/2020/93/CFC7 "Incidente Nº 93 - Querellante: FK., CE y otros imputado: M, F y otros s/incidente de nulidad", reg. 1055/2022, rta. 18/8/22.
Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].

[9] Cámara Federal de Casación Penal, Sala II.FLP 14624/2020/TO1/36/CFC10 "M, LD y otros s/ recurso de casación", reg. 1349/24, rta. 29/10/2024.
Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].

[10] Cámara Federal de Casación Penal, Sala II.FTU 48577/2013/TO1/CFC2, "S, CG s/recurso de casación", reg. 49/23, rta. 28/2/2023. Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].

casación"[11], al considerar que la ausencia de *hash* no invalidaba la legalidad de las escuchas si no se afectaba la confiabilidad del contenido.

En definitiva, la jurisprudencia mayoritaria —con base en el principio de sana crítica racional y en una concepción no ritualista de las nulidades— exige que se acredite una concreta vulneración de derechos fundamentales, en especial el derecho de defensa en juicio y el debido proceso. Tal como lo advirtió la Sala I en el caso "VC, E", "la mera afirmación de que la cadena de custodia no fue preservada [...] no alcanza para acreditar la invalidez pretendida".

Por lo tanto, una ruptura o manejo defectuoso de la cadena de custodia en evidencia digital puede —pero no necesariamente debe— implicar la nulidad de la prueba, debiendo evaluarse si tal afectación entra en tensión directa con derechos fundamentales emergentes, como la autodeterminación informativa, la privacidad digital o el derecho a no ser objeto de decisiones automatizadas sin control humano. La solución no es absoluta, sino contextual: depende del grado de afectación, la naturaleza del hecho investigado, la conducta procesal de las partes y la posibilidad o no de reconstrucción de la trazabilidad digital. Esta orientación implica una lectura funcional y compatible con los principios constitucionales, que evite tanto la arbitrariedad judicial como la impunidad por deficiencias meramente formales.

4.2 Jurisprudencia española y criterios de ponderación en la cadena de custodia digital

Por su parte también en España, uno de los puntos más controvertidos en torno al tratamiento procesal de la evidencia digital radica en determinar si toda afectación a la cadena de custodia debe traducirse necesariamente en una nulidad probatoria absoluta, o si, por el contrario, resulta posible —y deseable— aplicar un criterio de ponderación, caso por caso, que contemple el grado de afectación real sobre los derechos fundamentales involucrados.

La STC 170/2003[12], de 29 de septiembre, establece con claridad que no nos encontramos ante una mera formalidad legal, sino ante una garantía que se proyecta directamente sobre la validez constitucional de la prueba. En ese precedente, el Tribunal Constitucional sostuvo que la incorporación de soportes informáticos sin control judicial ni debidas garantías de custodia implicaba una vulneración del derecho a un proceso con todas las garantías, al quedar comprometida la integridad y autenticidad del material analizado. La

[11] Cámara Federal de Casación Penal, Sala I. FCT 12000054/2013/TO1/CFC8 "Y, DE y otros s/ recurso de casación", reg. 1167/19, rta. 12/7/2019. Disponible en: https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último acceso 02/10/2025].

[12] Tribunal Constitucional. (2003). STC 170/2003, rta 20/01/2003 disponible en https://www.poderjudicial.es/search/TS/openDocument/27bfc3b6dcabbc5a/20030703 [último acceso 02/10/2025].

falta de control jurisdiccional y el carácter regrabable de los soportes intervenidos resultaron, en ese caso, determinantes para declarar la nulidad probatoria.

No obstante, este enfoque coexiste con una línea jurisprudencial más matizada. Así, la decisión del Tribunal Supremo Español, STS 1349/2009[13], de 29 de diciembre, recuerda que la cadena de custodia no constituye en sí misma un derecho fundamental, sino un instrumento técnico de garantía. En esa línea, se afirma que la ruptura de la cadena no genera automáticamente una afectación constitucional, salvo que se utilice probatoriamente un elemento cuya autenticidad no pueda darse por acreditada y se haya menoscabado el derecho de defensa o el principio de contradicción. En palabras de la sentencia, "la irregularidad de la cadena de custodia no constituye, de por sí, vulneración de derecho fundamental alguno".

Este criterio ha sido reiterado en múltiples pronunciamientos posteriores. La STS 214/2020[14], por ejemplo, insiste en que "irregularidades de tipo burocrático, salvo que vayan acompañadas de otras deficiencias relevantes, no tienen por qué afectar la autenticidad de las evidencias". En similares términos, la STS 587/2014, de 18 de julio[15], aclara que la cadena de custodia no es prueba en sí misma, sino que sirve como garantía formal de la autenticidad de la prueba pericial. Su afectación incide sobre la verosimilitud del dictamen, no necesariamente sobre su validez.

Esta posición ha sido consolidada recientemente en la STS 1170/2024[16], de 19 de diciembre, donde se sostiene que "la nulidad o mejor dicho la inutilizabilidad de las evidencias no se deriva ni de cualquier irregularidad en el modo en que se conserven o se traten las evidencias ni de cualquier cortocircuito informativo sobre las distintas secuencias que integran el itinerario de su conservación y custodia a lo largo del proceso". En esta línea, se pone el foco en la lógica de la desconfianza y en la necesidad de contar con medios suficientes para que el tribunal pueda afirmar que la evidencia es genuina. Como criterio operativo, se subraya que los defectos en la documentación de la cadena afectan a la fiabilidad, pero no necesariamente a la validez.

[13]Tribunal Supremo (2009). STS 1349/2009, rta. 29/12/2009 disponible en https://www.poderjudicial.es/search/TS/openDocument/03b040811bed11cf/20100325 [último acceso 02/10/2025].

[14] Tribunal Supremo. (2020). STS 214/2020, rta 28/01/2020 disponible en https://www.poderjudicial.es/search/TS/openDocument/f23ea7461bd82757/20200210 [último acceso 02/10/2025].

[15] Tribunal Supremo. (2014). STS 587/2014, rta 18/02/2014 disponible en https://www.poderjudicial.es/search/TS/openDocument/075af59ec9196fc0/20140303 [último acceso 02/10/2025].

[16] Tribunal Supremo. (2024). STS 1170/2024, rta 29/02/2024 disponible en https://www.poderjudicial.es/search/TS/openDocument/8196c4d237f9a392a0a8778d75e36f0d/20240318 [último acceso 02/10/2025].

Desde el plano doctrinal, Jamardo Lorenzo (2025) propone una distinción fundamental entre la vertiente formal y la vertiente material de la cadena de custodia. La primera se refiere a los registros documentales que permiten reconstruir el trayecto de la prueba; la segunda, a los actos técnicos concretos de recolección, manipulación, transporte y análisis. Esta diferenciación permite graduar el impacto de cada eventual irregularidad: no es lo mismo una deficiencia de registro que una alteración sustancial del soporte o contenido probatorio (p. 315).

En términos similares, Figueroa Navarro (2011) define la cadena de custodia como una garantía de identidad, integridad y autenticidad que se mantiene cuando los vestigios han estado ininterrumpidamente a disposición de la autoridad judicial competente. Su afectación —más aún en el ámbito digital— no es una cuestión meramente formal, sino sustancial.

Ahora bien, el tratamiento procesal de la cadena de custodia en entornos digitales exige incorporar una dimensión adicional: el respeto a los derechos digitales emergentes. Una ruptura o manejo defectuoso de la cadena puede entrar en tensión directa no solo con el debido proceso y el derecho de defensa, sino también con derechos como la autodeterminación informativa, la protección de datos personales y el derecho a la intimidad digital. En efecto, tal como advierte el Tribunal Supremo en la STS 116/2025[17], la autenticidad del origen y la integridad del contenido son condiciones *sine qua non* para la valoración de cualquier prueba electrónica, especialmente en contextos como la mensajería instantánea, donde la manipulación de archivos o la suplantación de identidad son técnicamente viables.

El tratamiento deficiente de evidencias digitales, como ha señalado la jurisprudencia en la STS 287/2017[18], puede generar graves vacíos probatorios que afecten incluso la legitimidad del uso de dispositivos tecnológicos compartidos, donde el titular del derecho a la intimidad puede haberlo restringido tácitamente. El problema no radica solo en el contenido analizado, sino también en el contexto técnico y humano de adquisición, manipulación y conservación de la prueba. De ahí la necesidad de un análisis riguroso y situado.

En suma, la respuesta al interrogante planteado no puede ser unívoca. La jurisprudencia y la doctrina más recientes coinciden en que no toda afectación a la cadena de custodia comporta, por sí sola, una nulidad insanable. La clave reside en evaluar si esa afectación ha producido una quiebra real en las garantías esenciales del proceso, y si se han

[17] Tribunal Supremo. (2025). STS 116/2025, rta 21/01/2025 disponible en https://www.poderjudicial.es/search/TS/openDocument/b1f2f236ddff290da0a8778d75e36f0d/20250131 [último acceso 02/10/2025].

[18] Tribunal Supremo. (2017). STS 287/2017, rta 03/02/2017 disponible en https://www.poderjudicial.es/search/TS/openDocument/decfc2bd24b0750c/20170220 [último acceso 02/10/2025].

comprometido derechos fundamentales del imputado de forma sustancial. En este sentido, como recuerda la STS 372/2011[19], no basta con denunciar de forma genérica posibles manipulaciones, es necesario precisar en qué momento, cómo y con qué consecuencias se ha producido la ruptura. La cadena de custodia digital exige, por tanto, una doble mirada: una jurídica, orientada al control de legalidad y la defensa de garantías; y otra tecnológica, atenta a los riesgos de alteración, contaminación o suplantación en entornos vulnerables.

Antes bien, aunque Argentina y España convergen en rechazar una nulidad automática ante cualquier irregularidad, la jurisprudencia española ofrece un encuadre más nítidamente constitucional y una gramática operativa especialmente útil para la evidencia digital. A diferencia del enfoque argentino —que privilegia la verificación de perjuicio concreto y la reconstrucción técnico-probatoria del iter de la prueba—, España ancla el debate en dos pilares. Primero, la proyección constitucional de la cadena de custodia: la STC 170/2003 subraya que no es un rito vacío, sino una garantía que incide directamente en la validez de la prueba cuando faltan control judicial y salvaguardas de integridad del soporte. Segundo, una doctrina de proporcionalidad y suficiencia: la STS 1349/2009 y la STS 1170/2024 niegan que toda irregularidad implique inutilizabilidad; exigen medios que permitan al tribunal afirmar la genuinidad del material. En la misma línea, la STS 214/2020 y la STS 587/2014 distinguen entre defectos burocráticos —que erosionan fiabilidad— y quiebras materiales —que comprometen autenticidad—, mientras que la STS 372/2011 impone a quien alega la ruptura la carga de precisar cuándo, cómo y con qué consecuencias se produjo.

Esta lógica se ve reforzada por el énfasis en los derechos digitales: la STS 116/2025 exige acreditar origen auténtico e integridad del contenido —clave en mensajería instantánea— y la STS 287/2017 advierte sobre los riesgos contextuales (dispositivos compartidos, manipulación, suplantación). Así, ante la cuestión ¿qué aporta el derecho español al diálogo con la experiencia argentina? La respuesta es una perspectiva constitucional, un *test* de suficiencia probatoria centrado en autenticidad e integridad, y una metodología de graduación del defecto (formal vs. material) que evita el automatismo nulificante sin banalizar la garantía. Es una hoja de ruta práctica: documentar mejor, justificar técnicamente, y discutir la validez desde la confiabilidad verificable, no desde el mero ritualismo. Además, de incorporar al análisis la potencial afectación de derechos digitales y no solo garantías de derechos procesales.

[19] Tribunal Supremo. (2011). STS 372/2011. rta 25/01/2011 disponible en https://www.poderjudicial.es/search/TS/openDocument/32bcd2bd7a640572/20110224 [último acceso 02/10/2025].

Por otra parte, la determinación de quién debe acreditar la conservación adecuada de la cadena de custodia cobra especial relevancia cuando se trata de evidencias digitales, dada su fragilidad técnica y su alta susceptibilidad a alteraciones o manipulaciones no siempre detectables a simple vista. Este aspecto, si bien no ha sido objeto de una regulación sistemática en la legislación procesal penal, ha sido ampliamente abordado por la jurisprudencia y la doctrina, que han fijado criterios operativos aplicables al caso concreto.

4.3 La carga de la prueba y la trazabilidad de la evidencia digital

Tradicionalmente, la carga de la prueba en materia de legalidad y licitud de las pruebas recae sobre la parte que pretende su incorporación al proceso —generalmente, el órgano acusador—. Así lo confirma la STS 1170/2024, al señalar que "la parte que pretenda utilizar probatoriamente evidencias obtenidas en los primeros momentos de la investigación […] debe aportar aquellas informaciones que permitan acreditar su adecuada recogida, custodia y trazabilidad". Esta afirmación se articula con el principio de legalidad de la prueba y con la lógica epistémica que rige el proceso penal, conforme a la cual toda alegación fáctica debe ser respaldada por elementos probatorios confiables, sometidos al debido control judicial y contradicción de las partes.

En el mismo sentido, la STS 116/2025 destaca que cuando se trata de pruebas digitales —como mensajes de mensajería instantánea o archivos extraídos de dispositivos personales—, la parte que las introduce debe ofrecer todos los elementos que permitan acreditar no solo su origen, sino también su autenticidad e integridad. De hecho, en los supuestos en los que dicha prueba es impugnada por la defensa, se impone a la acusación la carga de proponer una pericia técnica adecuada que refuerce su validez, como reiteradamente ha establecido el Alto Tribunal. La sentencia precisa que "la impugnación de la autenticidad desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria", confirmando así un principio ya consolidado en el ámbito del derecho probatorio penal.

La jurisprudencia también ha advertido contra el uso estratégico de la ruptura de la cadena de custodia como argumento de defensa sin sustento objetivo. En la STS 214/2020, se recuerda que no basta una impugnación genérica para debilitar el valor probatorio de una evidencia: es necesario que la parte que cuestiona su validez precise con claridad el momento, la modalidad y la consecuencia concreta de la supuesta afectación. Esto mismo se refleja en la STS 287/2017, donde el Tribunal rechaza la alegación de una posible alteración del contenido informático con base en meras conjeturas, subrayando que "no basta con una reflexión genérica acerca de los riesgos potenciales de adulteración para desencadenar las dudas sobre su efectiva manipulación".

Este criterio responde a una lógica de equilibrio procesal: si bien corresponde inicialmente a quien introduce la prueba acreditar su licitud y autenticidad, también pesa sobre quien la impugna la carga mínima de argumentar y justificar técnicamente su objeción. La falta de participación de peritos de parte, la ausencia de contraanálisis técnico o la impugnación tardía —como se observó en la STS 116/2025— pueden debilitar seriamente la pretensión de nulidad.

Por su parte, la STS 372/2011 confirma que, incluso en ausencia de un modelo normativo unitario sobre cadena de custodia, el tribunal debe valorar si la información disponible —aunque no haya sido generada en condiciones ideales— es suficiente para excluir una alteración relevante de la prueba. La jurisprudencia insiste así en que la cadena de custodia es una garantía instrumental y que su infracción no genera automáticamente la invalidez del medio de prueba, salvo que se verifique una afectación concreta al contenido de lo analizado o a los derechos procesales fundamentales del imputado.

La cuestión cobra especial densidad en el terreno digital. El carácter editable y fácilmente manipulable de la información electrónica obliga a redoblar el estándar de diligencia exigible al órgano acusador. Herramientas como el código *hash* —aunque útiles para acreditar la integridad binaria—, resultan insuficientes si no van acompañadas de documentación que permita identificar quién, cómo y en qué contexto intervino sobre el dispositivo. De allí que, como señala la STS 208/2014[20], la regularidad de la cadena de custodia no es un simple formalismo, sino un presupuesto indispensable para la valoración de la prueba.

En síntesis, la doctrina jurisprudencial establece un sistema mixto de carga de la prueba en materia de cadena de custodia digital. Inicialmente, la carga de demostrar la licitud y autenticidad del material recae sobre la parte que lo introduce (generalmente, el Ministerio Público). Si la prueba es impugnada, corresponde a la parte que objeta aportar fundamentos concretos, pruebas técnicas alternativas o peritos de control. En última instancia, el tribunal debe ponderar la información disponible —más allá de formalidades— para decidir si existen dudas razonables sobre la integridad de la evidencia y, por tanto, sobre su valor probatorio.

Este modelo, lejos de debilitar las garantías procesales, fortalece el equilibrio entre eficacia penal y respeto a los derechos fundamentales. A su vez, permite una interpretación razonable del principio de legalidad probatoria en entornos digitales complejos, donde no todo error técnico puede traducirse en una exclusión automática,

[20] Tribunal Supremo. (2014). STS 208/2014, rta 28/01/2014 disponible en https://www.poderjudicial.es/search/TS/openDocument/f4bafc4a8486e5ad/20140211 [último acceso 02/10/2025].

pero tampoco debe pasar desapercibido cuando compromete la fiabilidad del material presentado como prueba.

Además, en el ámbito de la evidencia digital, donde la inmaterialidad de la prueba impone desafíos técnicos y jurídicos ineludibles, resulta imperioso preguntarse si la utilización exclusiva del código *hash* constituye, por sí sola, una garantía suficiente de integridad. La respuesta, lejos de admitir soluciones automáticas, exige una mirada crítica y situada en el contexto procesal y técnico en el que dicha herramienta es utilizada.

El Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en Ciberdelitos (Res. 234/2016 del Ministerio de Seguridad) y la Guía para la Obtención, Preservación y Tratamiento de Evidencia Digital de la Procuración General de la Nación (Res. 76/16) asignan al cálculo de *hash* un rol central: la verificación de inalterabilidad bit a bit de la copia forense respecto del original, así como la trazabilidad e identificación de los dispositivos intervenidos. Se trata de una función matemática unidireccional, que genera un identificador único para un contenido digital determinado, permitiendo así controlar su integridad sin revelar su contenido. En términos prácticos, el *hash* opera como una "huella digital" del archivo original.

No obstante, como lo ha reconocido en la causa “Y, D. E. y otros s/ recurso de casación”, resuelto por la Sala I de la CFCP, sostuvo que la sola ausencia de *hash* no invalida automáticamente la prueba digital, particularmente cuando la evidencia no admite modificaciones —como en el caso de grabaciones en discos compactos— y existen otros mecanismos de validación externa, tales como la procedencia legítima del soporte, el *test*imonio de los operadores intervinientes, y la trazabilidad administrativa del material.

Aún más clara es esta idea en la causa “D., L. P. y D., L. A. s/ recurso de casación”[21], donde la Sala I de la CFCP sostuvo que el *hash* es un instrumento útil pero no autosuficiente, en tanto su eficacia probatoria depende no solo de su correcta generación, sino también de su articulación con otros recaudos, como la conservación del soporte original. En esa causa, el tribunal cuestionó la prematura devolución de dispositivos, advirtiendo que, frente a futuros planteos de nulidad, el cotejo con el soporte físico original resultaba insustituible, incluso si existía una copia forense validada con *hash*. Este fallo confirma que la integridad no se agota en el resultado matemático, sino que incluye aspectos materiales y contextuales del procedimiento de adquisición y resguardo de la prueba.

Desde esta perspectiva, cabe afirmar que el código *hash* es una herramienta necesaria, pero no suficiente. Su valor como garantía depende de su generación en un entorno controlado, debidamente documentado, y en conjunción con otros mecanismos técnicos,

[21] Cámara Federal de Casación Penal, Sala I., D, L. P. y D, L. A. s/ recurso de casación, causa N° FMP 28852/2016/28/CFC1, Reg. 2135/19, rta. 04/12/2019, disponible en https://pjn-documento-api.pjn.gov.ar/api/documento/adjunto/200256 [último ingreso 02/10/2025].

tales como el uso de bloqueadores de escritura, la conservación del soporte original, y la intervención de peritos independientes. El *hash*, por sí solo, no impide que se planteen objeciones sobre la legitimidad del entorno de extracción, la manipulación previa al cálculo, o incluso la autenticidad del origen de la imagen forense.

En consecuencia, reducir la cadena de custodia digital a una función matemática equivale a vaciarla de su dimensión procesal. La integridad probatoria exige más que una coincidencia de cifras: requiere un sistema integral de garantías que incluya transparencia, trazabilidad, control jurisdiccional y condiciones técnicas verificables. Así lo reconoce también la jurisprudencia más reciente en el plano comparado, como la STS 1170/2024 en España, al sostener que "la inutilizabilidad de las evidencias no se deriva de cualquier irregularidad documental, sino de la imposibilidad de afirmar su autenticidad con medios suficientes".

Al respecto, Rubio Alamillo (2016) advierte que el cálculo del *hash*, para que sea válido, debe realizarse en condiciones técnicas controladas y sin que el dispositivo haya sido previamente conectado a otro sistema que pueda modificar su contenido. En el caso de dispositivos móviles, subraya que el aislamiento mediante jaula de Faraday es esencial para evitar comunicaciones externas que puedan comprometer la integridad de los datos. Solo bajo estas condiciones —afirma— puede sostenerse que el *hash* garantiza la conservación de la cadena de custodia en evidencias informáticas.

Esta afirmación se complementa con lo señalado por Contreras Calderón (2022), quien enfatiza la necesidad de proteger físicamente los dispositivos digitales desde su aprehensión. Para ello, detalla procedimientos concretos de embalaje, utilizando materiales como papel aluminio, cartón corrugado e icopor, destinados a aislar la evidencia de campos electromagnéticos, impactos y factores ambientales. Señala, además, que, en muchos contextos institucionales, las limitaciones materiales o presupuestarias llevan a improvisaciones que, aunque bienintencionadas, pueden vulnerar principios fundamentales de la cadena de custodia (pp. 7-8). De este modo, no solo se pone en riesgo la integridad de la evidencia, sino también su aptitud para ser valorada válidamente en el proceso penal.

En esta línea, González Reyes (2021) subraya que el proceso penal español carece de una normativa procesal que regule de manera clara y sistemática la recolección y conservación de evidencia electrónica, lo que obliga a depender de criterios técnicos extraídos de la práctica pericial. Para este autor, la combinación de dos elementos —la obtención de una copia forense o clonado del dispositivo y la aplicación de la función *hash*— constituye la única garantía técnica eficaz para asegurar la inalterabilidad del soporte digital intervenido. La falta de estas medidas mínimas compromete la validez de la prueba, pudiendo dar lugar, incluso, a su exclusión por lesionar el derecho fundamental a un proceso con todas las garantías (p. 78).

Ahora bien, la cuestión no reside únicamente en si el código *hash* es técnicamente confiable —lo cual, en términos binarios, lo es—, sino en el modo en que se obtiene y se acredita su generación ante el tribunal. Si no se documenta adecuadamente el momento, el entorno y las herramientas utilizadas para calcularlo, el valor probatorio del *hash* puede verse severamente disminuido. De ahí que la STS 1170/2024 insista en que no es la existencia del *hash* en sí lo que garantiza la integridad de la evidencia, sino el conjunto de circunstancias que permiten afirmar su autenticidad, como la trazabilidad, el control judicial, y la ausencia de manipulaciones constatables.

La jurisprudencia ha sido clara en establecer que la cadena de custodia digital no debe limitarse a la formalidad del *hash*, sino que debe permitir al órgano jurisdiccional reconstruir el trayecto completo del dispositivo o archivo desde su incautación hasta su análisis pericial. Como recuerda la STS 208/2014, la regularidad de la cadena de custodia constituye un presupuesto necesario para la valoración de la prueba, y su ruptura puede repercutir directamente sobre la fiabilidad y autenticidad del elemento de convicción.

Por tanto, el uso del *hash* como única medida de garantía puede resultar insuficiente si no se encuentra enmarcado en un procedimiento integral de conservación técnica, adecuadamente documentado y respaldado por protocolos claros. Como advierte González Reyes (2021), la falta de control judicial y de garantías sobre la identidad e integridad de la prueba digital no es un defecto meramente procesal: puede implicar una lesión a derechos constitucionales, particularmente cuando se incorpora al proceso material electrónico sin haber verificado debidamente su origen o contenido (p. 79).

En definitiva, debe rechazarse la idea de que el *hash*, por sí solo, puede suplir la ausencia de una cadena de custodia debidamente preservada. El contexto técnico de su obtención, el estado del dispositivo, los procedimientos de aislamiento, el control de acceso y la existencia de documentación verificable son elementos imprescindibles para que esa huella digital cumpla realmente su función de garantía. La fiabilidad del *hash* no puede desvincularse de su entorno operativo, y es en esa interacción donde se define —en última instancia— la legitimidad probatoria de la evidencia digital.

5. ANÁLISIS SOBRE LOS APORTES DE LA JURISPRUDENCIA COMPARADA

Desde una mirada comparativa, la jurisprudencia española aporta elementos conceptuales y metodológicos relevantes que enriquecen la reflexión argentina sobre los alcances y límites del código *hash* en la cadena de custodia digital. Si bien ambos sistemas coinciden en considerar al *hash* una herramienta técnica valiosa para verificar la inalterabilidad de una copia forense, España ha desarrollado una doctrina más sistemática en torno a su insuficiencia como único mecanismo de garantía.

Mientras que la jurisprudencia argentina, como se observa en la causa "Y, D. E. y otros s/ recurso de casación", se reconoce que la ausencia de *hash* no invalida la prueba si existen otras condiciones que preservan su autenticidad —como el soporte físico, la intervención de personal autorizado y la trazabilidad administrativa—, la jurisprudencia española, en particular la STS 1170/2024, advierte que no es la mera existencia del *hash* lo que garantiza la integridad, sino el conjunto de circunstancias que permiten verificar que su obtención fue realizada en un entorno técnico controlado, sin manipulaciones previas y con adecuada documentación.

Esta diferencia de enfoque no es meramente terminológica. En el sistema español, se ha puesto especial énfasis en la necesidad de que el *hash* esté vinculado a un proceso formal y materialmente garantizado. En este sentido, la jurisprudencia española introduce una dimensión ambiental y operativa que enriquece el análisis tradicional centrado exclusivamente en la matemática del *hash*.

Además, el tratamiento doctrinal en España ha propuesto distinciones conceptuales que aún no han sido plenamente sistematizadas en el plano argentino. Tal es el caso de la diferenciación entre la vertiente formal y la vertiente material de la cadena de custodia, propuesta por Jamardo Lorenzo (2025, p. 315) y antes expuesta. Este esquema permite discernir si una irregularidad afecta únicamente el registro documental o si compromete, de modo sustancial, el soporte mismo de la prueba. Esta herramienta analítica podría resultar de gran utilidad para los operadores judiciales argentinos ante planteos de nulidad que se basen exclusivamente en omisiones técnicas como la falta de *hash*.

Por último, el sistema español ha logrado consolidar una advertencia clave: la confianza ciega en el *hash* puede generar una falsa presunción de integridad si no va acompañada de controles reales y verificables sobre el entorno de adquisición. En este sentido, la jurisprudencia española invita al sistema argentino a reforzar la documentación del contexto técnico de la pericia, a profesionalizar la intervención forense desde el inicio mismo de la cadena, y a integrar una perspectiva más amplia sobre lo que significa preservar la integridad de un dato digital.

Esta necesidad de ampliar la mirada ha sido también destacada en la doctrina argentina. Cistoldi, Di Iorio y Rosales (2025) sostienen que la irrupción de los ciberdelitos y la multiplicación de fuentes de prueba digital impone no solo renovar saberes técnicos, sino también evitar el aislamiento entre el derecho y las disciplinas forenses. En esta línea, proponen la aplicación de los "criterios Daubert" a la prueba digital, siguiendo principios forenses como evitar la contaminación, controlar la trazabilidad y actuar metódicamente. Particular énfasis se pone en que la trazabilidad no se reduce al estado de los dispositivos,

sino que debe documentarse de forma auditable, repetible, reproducible y justificable (p. 755, pp. 788-789)[22].

Desde esta óptica, la cadena de custodia debe evolucionar hacia una "cadena de valor", en la que no solo se preserve la identidad e integridad del soporte, sino que se garantice la legitimidad técnica del procedimiento en su conjunto. Esta reformulación es coherente con lo señalado por la Procuración General del MPBA en su Resolución 889/15, que reconoce la necesidad de ajustar el instrumento de cadena de custodia al carácter intangible de la prueba digital.

Por su parte, la jurisprudencia española también ha vinculado esta exigencia técnica con principios sustanciales del proceso penal. En palabras de Velasco Núñez (2025), el clonado y el *hash* no deben entenderse como simples formalidades, sino como garantías para que lo que se analiza sea estrictamente lo que se ocupó, evitando dudas por alteraciones o manipulaciones. Asimismo, advierte que, si bien la copia puede bastar para preservar el contenido, la ocupación del dispositivo físico puede ser necesaria cuando este constituye en sí mismo un objeto del delito o cuando representa la única vía para garantizar una pericia adecuada. De allí que se recomiende no devolver el soporte hasta verificar la fiabilidad del clonado, y que el mismo se ponga a disposición de la defensa para el ejercicio pleno del derecho de contradicción y para facilitar el acceso al contenido (pp. 258-259).

En suma, los desarrollos jurisprudenciales y doctrinales de España no solo confirman la importancia del *hash* como herramienta de control, sino que insisten en que su eficacia depende de un entramado técnico, procesal y documental que lo sustente. Este enfoque, compatible con los principios del debido proceso y del derecho a la defensa, representa un aporte sustancial al tratamiento de la evidencia digital en el ámbito argentino, en particular ante los desafíos que impone el manejo de información electrónica en contextos judiciales cada vez más complejos y técnicamente exigentes.

6. CONCLUSIONES

La nulidad por ruptura de cadena de custodia digital no es automática, sino contextual: tanto en la jurisprudencia argentina como española, se exige demostrar un perjuicio concreto o una afectación sustancial a derechos fundamentales —como el derecho de defensa o la autenticidad probatoria— para que la invalidez procesal sea procedente.

[22] Estos criterios fueron establecidos por la Corte Suprema de Justicia de los Estados Unidos, en el caso *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). Dichos parámetros —no taxativos— orientan la evaluación judicial de la fiabilidad científica de la prueba pericial, considerando factores como la verificabilidad empírica, la revisión por pares, la tasa de error conocida y la aceptación general en la comunidad científica.

El código *hash* es una herramienta técnica necesaria, pero no suficiente: su eficacia como mecanismo de garantía depende del contexto técnico de su generación, incluyendo el uso de bloqueadores de escritura, el aislamiento del dispositivo, la documentación verificable y la trazabilidad de todo el procedimiento pericial.

La intervención sin control judicial ni garantías mínimas de integridad puede comprometer la validez constitucional de la prueba: así lo establece la doctrina jurisprudencial española (e.g. STC 170/2003 y STS 1170/2024), recordando que la cadena de custodia no es un simple formalismo, sino una condición de legitimidad procesal.

La jurisprudencia argentina tiende a ponderar caso por caso, mientras que España articula una perspectiva más sistemática y constitucional: el enfoque argentino privilegia el análisis del perjuicio concreto y de la trazabilidad recuperable, en tanto que el derecho español introduce distinciones entre irregularidades formales y sustanciales, vinculadas a la autenticidad y confiabilidad de la prueba.

La prueba digital impone nuevos estándares técnicos y epistemológicos en el proceso penal: a la luz de principios como los criterios de Daubert, propuestos por la jurisprudencia, resulta imprescindible reformular la cadena de custodia como una "cadena de valor", basada en procedimientos auditables, repetibles, reproducibles y justificables, que aseguren tanto la integridad como la transparencia en el tratamiento probatorio de datos electrónicos.

BIBLIOGRAFÍA

Cistoldi, P. A., Di Iorio, A. H., & Rosales, M. F. (2025). Prueba digital: De la cadena de custodia a la cadena de valor. En D. Dupuy (Ed.), *Tratado internacional sobre procedimiento criminal, transnacional y digital* (pp. 753–800). Tirant Lo Blanch.

Contreras Calderón, C. A. (2022). Buenas prácticas en informática forense para el procesamiento de evidencia digital o información electrónicamente almacenada. *Publicaciones e Investigación, 15*(2). https://doi.org/10.22490/25394088.5245.

EUROPOL (2025). Evaluación de la Amenaza de la Delincuencia Organizada en Internet (IOCTA). Disponible en: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data.

Figueroa Navarro, C. (2011). El aseguramiento de las pruebas y la cadena de custodia. *La Ley Penal*, (84), julio.

González Reyes, J. M. (2021). La prueba pericial digital y la cadena de custodia. *Anales de la Facultad de Derecho*, 38, 43–79. https://doi.org/10.25145/j.anfade.2021.38.03.

Jamardo Lorenzo, A. (2025). La dimensión tecnológica de la cadena de custodia: algunas claves. InDret 2, 298-345. https://indret.com/la-dimension-tecnologica-de-la-cadena-de-custodia-algunas-claves/.

Rubio Alamillo, J. (2016). Conservación de la cadena de custodia de una evidencia informática. *Diario La Ley*, (8859), Sección Doctrina, 9 de noviembre. Wolters Kluwer.

Velasco Núñez, E. (2025). Registro (estático y dinámico) de dispositivos de almacenamiento masivo de datos. En D. Dupuy (Ed.), *Tratado internacional sobre procedimiento criminal, transnacional y digital* (pp. 239–297). Tirant Lo Blanch.