Inteligencia de fuentes abiertas (OSINT) y motivación judicial: un estándar tridimensional para la prueba penal

Open-Source Intelligence (OSINT) and Judicial Reasoning: A Three-Dimensional Standard for Evidence in Criminal Proceedings

Wendy Requejo-Passoni[1]
Universidad Científica del Sur, Lima, Perú
wrequejo@cientifica.edu.pe
https://orcid.org/0000-0001-9952-2199

Resumen: El empleo de inteligencia de fuentes abiertas (OSINT) en la investigación penal permite localizar, preservar, relacionar y analizar información digital públicamente accesible. Cuando ese proceso incorpora inteligencia artificial, la aparente objetividad del resultado puede ocultar decisiones sobre selección de datos, autenticidad, correlación y atribución. En este marco, la pregunta que guía la investigación es la siguiente: ¿qué razones debe expresar el órgano judicial al admitir, valorar o excluir un informe OSINT asistido por inteligencia artificial para que su decisión sea controlable y compatible con el derecho de defensa? Mediante una metodología jurídico-dogmática y de reconstrucción argumentativa, complementada con casos de Argentina, España y la justicia penal internacional, se distingue entre fuente, preservación, transformación analítica e informe. Se sostiene que la ratificación del analista y la referencia genérica a protocolos técnicos no bastan para justificar la decisión. Como contribución, se propone un estándar tridimensional de justificación judicial, integrado por la legitimidad de la obtención y utilización, la fiabilidad epistémica y la contradicción

[1] Profesora Tiempo Parcial en la Universidad Científica del Sur, Lima, Perú. Máster en Derecho Penal por la Universidad de Salamanca y Máster en Derecho de la Ciberseguridad y Entornos Digitales por la Universidad de León. Doctora en Derecho por la Universidad de Salamanca.

efectiva. Finalmente, se formula una respuesta graduada frente a sus defectos: subsanación, necesidad de corroboración, reducción del peso probatorio o exclusión, según su naturaleza e incidencia.

Palabras clave: OSINT; prueba digital; motivación judicial; inteligencia artificial; proceso penal.

Abstract: *The use of open-source intelligence (OSINT) in criminal investigations makes it possible to locate, preserve, connect, and analyse publicly accessible digital information. When this process incorporates artificial intelligence, the apparent objectivity of its output may conceal decisions concerning data selection, authenticity, correlation, and attribution. Within this framework, the research is guided by the following question: what reasons must a court provide when admitting, assessing, or excluding an AI-assisted OSINT report to ensure that its decision is reviewable and compatible with the right of defence? It adopts a legal-dogmatic and argumentative reconstruction methodology, supplemented by cases from Argentina, Spain, and international criminal justice, and distinguishes among the source, its preservation, analytical transformation, and the resulting report. It argues that the analyst's testimony and a generic reference to technical protocols are insufficient to justify the judicial decision. The article proposes a three-dimensional standard for judicial justification comprising the legitimacy of obtaining and using the information, epistemic reliability, and effective adversarial scrutiny. It then develops a graduated response to defects: remediation, corroboration, reduced evidentiary weight, or exclusion, depending on their nature and impact.*

Keywords: *OSINT; digital evidence; judicial reasoning; artificial intelligence; criminal proceedings.*

Contenido: Introducción; 1. OSINT como objeto de decisión probatoria; 1.1. Del acceso público a la obtención de evidencia; 1.2. Preservación y cadena de inferencia; 1.3. Transformación analítica y automatización; 2. De las salvaguardas internacionales al deber de motivación; 2.1. El alcance limitado de los instrumentos sobre ciberdelincuencia; 2.2. Proceso justo y motivación probatoria; 3. Naturaleza procesal del informe OSINT y límites de la ratificación del analista; 4. Un estándar tridimensional de justificación judicial; 4.1. Legitimidad; 4.2. Fiabilidad epistémica; 4.3. Contradicción efectiva; 5. Defectos y consecuencias procesales; Conclusiones; Referencias.

Introducción

La expansión de las tecnologías de la información ha desplazado una parte relevante de los rastros asociados con el delito hacia entornos digitales. Fotografías, vídeos, perfiles, publicaciones, mapas, metadatos y relaciones entre usuarios se encuentran en páginas web, redes sociales y repositorios accesibles a través de internet. En ese contexto, la inteligencia de fuentes abiertas (*Open Source Intelligence*, OSINT) permite convertir información dispersa en conocimiento útil para identificar personas, reconstruir acontecimientos o contrastar hipótesis dentro de una investigación penal.

En este sentido, Sampson advierte que seguir las «migas de pan» (*breadcrumbs*) dejadas por las interacciones digitales para localizar personas, patrones o bienes es distinto de utilizar ese material para sustentar una acusación penal, ya que la inteligencia y la evidencia cumplen finalidades diferentes[2], aunque en el ciberespacio esa distancia se reduce y sus fronteras tienden a difuminarse.

En efecto, que un dato sea técnicamente accesible no resuelve su legitimidad jurídica ni determina su fiabilidad probatoria. La recopilación sistemática, la conservación prolongada y la correlación de datos fragmentarios pueden revelar desplazamientos, vínculos personales o patrones de comportamiento que no serían visibles mediante una observación aislada. Asimismo, la fuente abierta puede ser falsa, haber sido manipulada o aparecer fuera de contexto. Por ello, el tránsito desde la información disponible en internet, recopilada mediante técnicas de inteligencia, hasta su utilización en una decisión penal exige someterla a los estándares forenses y procesales aplicables a cualquier evidencia[3]. Esto requiere examinar tanto su admisibilidad como su peso probatorio[4] y, en particular, su obtención, preservación, método y las inferencias formuladas a partir de ella.

---

2 SAMPSON (2016), p. 296-297.

3 SAMPSON (2016), p. 302.

4 GHIONI-TADDEO-FLORIDI (2024), p. 1836; en el mismo sentido, WINTER (2025), p. 10.

El problema se intensifica cuando el análisis incorpora inteligencia artificial (IA). No toda investigación OSINT utiliza IA ni todas las operaciones automatizadas presentan el mismo riesgo. Una herramienta puede ordenar resultados, transcribir audios o detectar coincidencias; otra puede reconocer rostros, vincular identidades o asignar puntuaciones de similitud. En cada caso, la automatización interviene en un punto distinto de la cadena inferencial y condiciona de manera diferente la posibilidad de comprender y controvertir el resultado.

Las categorías probatorias tradicionales ofrecen respuestas parciales. La fuente digital puede incorporarse como documento; la validación técnica o la geolocalización pueden requerir conocimiento experto; y quien efectuó la búsqueda puede declarar sobre lo que observó. Ninguna de esas categorías, por sí sola, garantiza que el tribunal conozca las fuentes empleadas, reconstruya las transformaciones realizadas o examine las explicaciones alternativas. La comparecencia de quien firma el informe tampoco reemplaza la documentación de un trabajo distribuido entre investigadores, herramientas y sistemas que esa persona quizá no controla íntegramente.

Por tanto, la pregunta central de este trabajo es ¿qué razones mínimas debe expresar el órgano judicial al admitir, valorar o excluir un informe OSINT asistido por IA? Se adopta como hipótesis que la ratificación personal del analista y la invocación genérica de estándares técnicos son insuficientes, y que la decisión debe justificar tres dimensiones interrelacionadas: la legitimidad de la obtención y utilización de la información, la fiabilidad epistémica del recorrido que conecta las fuentes con la conclusión y la existencia de una contradicción efectiva.

La propuesta no constituye un nuevo estándar de prueba ni fija el umbral para condenar, sino que se trata de un estándar tridimensional de justificación judicial que permite identificar las cuestiones que la decisión debe hacer explícitas antes de atribuir fuerza probatoria al informe. Desde luego, su profundidad será variable y dependerá de la función del material, de la complejidad técnica, de su peso dentro de la hipótesis acusatoria y de las objeciones formuladas por las partes.

La investigación adopta una metodología jurídico-dogmática y de reconstrucción argumentativa. Se sustenta conceptualmente en la teoría racionalista de la prueba, las garantías del proceso justo, la

literatura contemporánea sobre información digital de fuentes abiertas y los estándares técnicos de preservación. Por su parte, los casos de Argentina, España y la justicia penal internacional cumplen una función ilustrativa y comparada y no constituyen una muestra empírica destinada a medir la frecuencia de los defectos, ni se emplean para afirmar que las consecuencias procesales sean idénticas en los distintos ordenamientos. Cabe precisar que el estándar propuesto tampoco se presenta como una regla suprapositiva, sino como una pauta de justificación cuya aplicación y consecuencias deben concretarse conforme al derecho positivo vigente en cada sistema procesal.

El análisis se desarrolla en cinco apartados. El primero diferencia las capas que componen un producto OSINT y sus principales riesgos. El segundo precisa la aportación y los límites de las salvaguardas internacionales sobre evidencia electrónica. El tercero examina la función del analista. El cuarto formula el estándar tridimensional de justificación judicial. El quinto gradúa las consecuencias procesales de sus defectos.

1. OSINT como objeto de decisión probatoria

Es menester esclarecer que OSINT no designa un medio de prueba autónomo ni una herramienta determinada, sino un proceso orientado a localizar, obtener, preservar, contrastar y analizar información procedente de fuentes abiertas para producir conocimiento relevante respecto de una finalidad.

En el ámbito de la justicia internacional existe una tradición consolidada en el uso de la *Digital Open-Source Information* (DOSI), concepto que pone el acento en los materiales digitales disponibles públicamente y evita confundirlos con el producto de inteligencia elaborado a partir de ellos[5]. Sin embargo, también es empleada por misiones de investigación de la ONU, organizaciones de derechos humanos, periodistas y tribunales nacionales en casos de jurisdicción universal[6]. En suma, la

[5] GILLETT-FAN (2023), p. 661-662.

[6] GILLETT-FAN (2023), p. 663.

evidencia de fuentes abiertas se ha consolidado como información con valor probatorio[7].

No obstante, su complejidad interna exige distinguir con precisión las distintas capas que la componen, a fin de identificar los problemas que pueden presentarse durante la motivación judicial[8]. La primera está constituida por la fuente digital original. La segunda comprende los actos de localización y recopilación. La tercera se refiere a la preservación del contenido y sus metadatos. La cuarta incorpora las operaciones de verificación, correlación y análisis. La última corresponde al informe, gráfico o conclusión que se incorpora al proceso. La declaración del analista constituye un elemento adicional, pues permite interrogar a una persona acerca de las tareas que realizó, pero no sustituye las fuentes ni la documentación del método.

Esta separación evita dos confusiones particularmente relevantes. Por un lado, la autenticidad de un archivo no demuestra la verdad de su contenido. A su vez, la integridad de una copia tampoco acredita la corrección de la inferencia elaborada a partir de ella. Por ello, la decisión judicial debe identificar cuál de estas capas se encuentra en discusión y qué función cumple dentro del razonamiento probatorio.

1.1. Del acceso público a la obtención de evidencia

En principio, la actuación estatal puede partir de una sospecha individualizada o de una búsqueda preventiva. En el primer supuesto, la autoridad consulta redes sociales u otras plataformas para obtener información vinculada con una investigación determinada. En el segundo,

---

[7] OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 6.

[8] Por su parte, el Protocolo identifica seis fases principales del proceso: consulta en línea, evaluación preliminar, recopilación, preservación, verificación y análisis de investigación. Estas fases describen la secuencia operativa de la investigación OSINT, a diferencia de las cinco capas aquí propuestas, que no aluden a un orden de actuación sino a los distintos elementos de la cadena probatoria relevantes para la motivación judicial. OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 53.

selecciona palabras clave, comportamientos o perfiles para detectar hechos todavía no individualizados. Esta diferencia resulta especialmente relevante, ya que el monitoreo general puede condicionar todo el itinerario procesal aun cuando su resultado no sea presentado después como una prueba autónoma.

Por ejemplo, el caso argentino de Kevin Guerra permite ilustrar este riesgo[9]. Una búsqueda policial basada en términos predeterminados detectó una expresión irónica publicada durante el confinamiento y originó una investigación penal. Si bien el proceso terminó con el sobreseimiento, puso de manifiesto que la sola referencia al ciberpatrullaje no responde a las preguntas sobre la habilitación, la finalidad y los límites de la vigilancia.

Ante los riesgos derivados de la vigilancia masiva, y siguiendo a Winter, corresponde someter las técnicas de recopilación y análisis de información a un marco reforzado de garantías[10]. Para tal propósito, no basta con afirmar que la información «estaba en internet». Una publicación puede ser visible para cualquier usuario y, no obstante, su recopilación masiva, su tratamiento en una base de datos y su combinación con otras fuentes pueden modificar cualitativamente la intervención. En particular, la agregación puede producir un «efecto mosaico» (*mosaic effect*), mediante el cual datos aparentemente inocuos permiten, al ser analizados en conjunto, reconstruir identidades, movimientos, vínculos o preferencias[11], escenario especialmente problemático para la privacidad y la libertad de expresión; derechos que conservan su protección en el espacio digital conforme a los artículos 17 y 19 del Pacto Internacional de Derechos Civiles y Políticos y a los artículos 8, 11, 13 y 25 de la Convención Americana sobre Derechos Humanos[12].

---

[9] En abril de 2020, durante el confinamiento por la COVID-19, un joven de 21 años de Balcarce publicó en Twitter un mensaje en el que preguntaba irónicamente si continuaba en pie un posible saqueo ante la falta de pago del bono de 10 000 pesos. La publicación fue identificada por la Subdirección de Delitos Tecnológicos de la Gendarmería Nacional mediante un sistema automatizado de ciberpatrullaje basado en las palabras clave «saquear», «cuarentena» y «Argentina». CELS (2021).

[10] WINTER (2025), p. 5.

[11] GHIONI-TADDEO-FLORIDI (2024), p. 1836.

[12] NACIONES UNIDAS (1966), arts. 17 y 19; ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (1969), arts. 8, 11, 13 y 25.

Por ello, la motivación debe explicar qué obtuvo la autoridad, mediante qué procedimiento, durante cuánto tiempo, con qué volumen, respecto de qué personas y para qué finalidad. Asimismo, debe examinar las barreras de acceso, las medidas de minimización y la eventual afectación de terceros. La posibilidad técnica de observar una fuente constituye, en suma, únicamente el inicio del análisis.

1.2. Preservación y cadena de inferencia

Otro aspecto que considerar es que la información digital es volátil y susceptible de manipulación[13]. Una publicación puede modificarse, desaparecer, perder metadatos o ser presentada de modo distinto por la plataforma. De ahí que, en el contexto de una investigación forense digital, su preservación deba registrar, según las características del caso, la dirección, la fecha y hora de acceso, el método de captura, el contenido completo, los metadatos disponibles, las herramientas empleadas y las transformaciones posteriores[14].

En esta línea, el Protocolo de Berkeley sistematiza buenas prácticas para las investigaciones digitales de violaciones del derecho penal internacional, los derechos humanos y el derecho humanitario. Aunque no determina por sí mismo la admisibilidad en los procesos nacionales, su utilidad reside en traducir la fiabilidad en comprobaciones concretas, entre ellas, planificar la recopilación[15], conservar los materiales originales[16],

---

[13] JAMARDO LORENZO (2025), p. 315.

[14] Sobre el proceso detallado de la investigación forense, véase RAGHAVAN (2013), p. 92-93.

[15] OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 43.

[16] OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 61.

documentar las transformaciones[17], registrar las herramientas[18] y asegurar la trazabilidad del procedimiento[19].

Ahora bien, describir la cadena de custodia del informe OSINT no es suficiente para dotar de contenido a la motivación de una decisión en un proceso penal, ya que solo permite reconstruir el tratamiento del material desde su obtención, más no explicar cómo se pasó de ese material a una conclusión sobre identidad, localización, vínculo o autoría. A modo de ejemplo, un código *hash* puede confirmar que dos archivos son binariamente idénticos[20], pero no demuestra que el perfil perteneciera a una persona, ni que el contenido fuese auténtico antes de su captura ni que su interpretación sea correcta[21].

Será menester, tal como apunta Ferrer Beltrán, que la estructura recursiva del razonamiento probatorio confeccione una cadena inferencial, en la que una conclusión parcial se convierte en la premisa del paso siguiente[22]. Así, si la atribución de una cuenta se apoya en una fotografía y esa atribución permite después situar al acusado en un lugar, el tribunal debe examinar ambos enlaces y no solamente la integridad del archivo final.

Por otra parte, los asuntos *Al Mahdi* y *Al-Werfalli* ante la Corte Penal Internacional muestran que la información abierta puede cumplir funciones diferentes. En el primero, los materiales geoespaciales, las imágenes satelitales, las fotografías y los vídeos contribuyeron a organizar y presentar los hechos de Tombuctú. En el segundo, los vídeos difundidos en redes sociales ocuparon un lugar central y fueron contextualizados

---

17 OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 59.

18 OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 11.

19 OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS-HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (2022), p. 5.

20 RAGHAVAN (2013), p. 92.

21 FISBERG (2025), p. 10-11.

22 FERRER BELTRÁN (2020), p. 378.

mediante geolocalización e imágenes satelitales[23]. Por tanto, la intensidad de la motivación también debe atender a la función concreta atribuida al material, ya sea presentar, corroborar o sostener una inferencia decisiva.

1.3. Transformación analítica y automatización

En plena tercera década del siglo XXI, la capacidad operativa de OSINT se ha beneficiado considerablemente de sistemas de IA que pueden intervenir en la selección, clasificación, transformación o interpretación de las fuentes. Sin embargo, el reconocimiento facial, la traducción automática, la transcripción, la detección de objetos, el análisis de vínculos y la comparación de ubicaciones no son operaciones equivalentes. Cada una depende de datos, umbrales y decisiones de configuración capaces de producir falsos positivos o amplificar sesgos. A los efectos de este trabajo, un informe OSINT se considera asistido por IA cuando, durante su elaboración, un sistema produce resultados (como clasificaciones, coincidencias, predicciones, transcripciones o contenido) que inciden en la selección, verificación, correlación o interpretación de las fuentes. No basta, por tanto, el uso de software convencional para buscar, capturar, almacenar o preservar información: la asistencia mediante IA exige que la salida del sistema intervenga en alguna fase relevante del recorrido que conduce desde las fuentes hasta la conclusión.

Por ello, la alusión genérica a una «caja negra» resulta tan insuficiente como la confianza automática en la tecnología. Ciertamente, la decisión debe identificar qué operación fue automatizada, qué función cumplió en la conclusión y qué intervención humana existió, lo que evidencia una complejidad derivada de su propia infraestructura que, para ser auditada, requiere de grandes esfuerzos en tiempo y recursos, tal como apuntan Ghioni, Taddeo y Floridi[24].

Ello no significa que el tribunal deba conocer el código fuente en todos los casos. No obstante, sí debe disponer de información suficiente sobre la herramienta, su versión, la operación realizada, los datos de

---

[23] TREVISAN (2021), p. 11-13.

[24] GHIONI-TADDEO-FLORIDI (2024), p. 1838.

entrada, sus limitaciones conocidas y la supervisión humana. Cuando una salida algorítmica se incorpora sin hacer comprensible el recorrido que conduce a ella, se debilitan tanto la motivación como la posibilidad de impugnación[25].

2. De las salvaguardas internacionales al deber de motivación

2.1. El alcance limitado de los instrumentos sobre ciberdelincuencia

La obtención de evidencia electrónica se encuentra regulada por dos instrumentos internacionales especialmente relevantes. Por un lado, el Convenio de Budapest. Por otro lado, la Convención de las Naciones Unidas contra la Ciberdelincuencia. Los artículos 14 y 15 del primero someten las potestades de investigación a las condiciones previstas por el derecho interno, la protección de los derechos humanos, la proporcionalidad y, según la medida, el control judicial o independiente, los motivos justificativos y los límites de alcance y duración. Los artículos 23 y 24 de la Convención de las Naciones Unidas siguen una estructura semejante e incorporan expresamente la necesidad de un recurso efectivo.[26]

Conviene puntualizar que la situación jurídica de ambos instrumentos no es idéntica. El Convenio de Budapest se encuentra en vigor. La Convención de las Naciones Unidas fue adoptada el 24 de diciembre de 2024 y abierta a la firma en Hanói el 25 y 26 de octubre de 2025, pero a la fecha de cierre de este trabajo todavía no había entrado en vigor. Por esta razón, su artículo 24 debe tratarse como la expresión de una convergencia internacional emergente y no como una regla convencional directamente aplicable en todos los ordenamientos[27].

Con todo, tampoco toda actividad OSINT constituye una potestad sometida directamente a estas disposiciones. Una consulta manual y

---

[25] MOLINA (2022), p. 147.

[26] CONSEJO DE EUROPA (2001), arts. 14-15; NACIONES UNIDAS (2024), arts. 23-24.

[27] NACIONES UNIDAS (s/f), estado al 29 jul. 2026.

puntual en una página genuinamente pública puede quedar fuera de su ámbito inmediato. La situación es distinta cuando se utilizan órdenes de producción, conservación obligatoria, acceso a contenidos restringidos, identidades encubiertas, interceptación u otras potestades reguladas. En estos supuestos, la denominación OSINT no puede ocultar la intensidad real de la actuación.

A su vez, ni el artículo 15 del Convenio de Budapest ni el artículo 24 de la Convención de las Naciones Unidas regulan la autenticidad, la reproducibilidad, el funcionamiento de los sistemas de IA o la fuerza probatoria de un informe. Su contribución se concentra en la legitimidad de la obtención y utilización. Reconocer este límite no debilita su utilidad, sino que evita deducir un marco de valoración probatoria de instrumentos concebidos para otro propósito.

De ahí que resulte necesario distinguir tres momentos. El primero corresponde a la autorización de la medida, en la que se examinan de forma prospectiva la base jurídica, la finalidad, la necesidad, la proporcionalidad, el alcance y la duración. El segundo se refiere a su ejecución, que debe mantenerse dentro de los límites autorizados. El tercero surge cuando el resultado se incorpora al proceso y debe decidirse sobre su admisión o peso probatorio. Esta distinción permite advertir que una medida correctamente autorizada puede producir un resultado poco fiable y que, a la inversa, un informe técnicamente correcto puede provenir de una injerencia ilegítima.

Las salvaguardas convencionales se proyectan, por tanto, sobre la decisión probatoria de una forma limitada pero relevante. Cuando el informe procede de una potestad regulada, el tribunal no debe separarlo artificialmente del procedimiento que lo produjo, sino identificar la base jurídica, la autoridad competente, la finalidad, el alcance y la eventual afectación de terceros. En todo caso, la consecuencia de una vulneración dependerá del derecho interno y de su incidencia sobre los derechos y la fiabilidad.

2.2. Proceso justo y motivación probatoria

La fundamentación de la decisión sobre un informe OSINT debe completarse con las garantías generales del proceso justo. El artículo 14 del Pacto Internacional de Derechos Civiles y Políticos, los artículos 8

y 25 de la Convención Americana y el artículo 6 del Convenio Europeo de Derechos Humanos sustentan el derecho a conocer y controvertir los elementos esenciales de la decisión. Si bien estos instrumentos no contienen un listado técnico para valorar OSINT, exigen una decisión racional, revisable y compatible con el derecho de defensa.

Como antes se afirmó, desde una concepción racionalista de la prueba expuesta por Ferrer Beltrán, motivar no equivale a enumerar las evidencias, sino que la resolución debe exteriorizar por qué considera acreditada la procedencia del material, por qué confía en el método, por qué acepta la inferencia propuesta y por qué descarta las alternativas relevantes[28]. Así, la motivación permite controlar el razonamiento y reduce el riesgo de que la autoridad técnica sustituya a la valoración judicial.

La problemática se intensifica cuando, pese a haber recibido formalmente el informe, la defensa no puede examinar las herramientas, los registros o los elementos técnicos que sustentan sus conclusiones. En tales condiciones, una resolución comprensible cumple una doble función. Por un lado, obliga al tribunal a someter a control las premisas del informe. Paralelamente, permite impugnar la decisión mediante los recursos correspondientes. Sin acceso efectivo al recorrido que une las fuentes con la conclusión, la contradicción quedaría reducida a una posibilidad meramente formal.

Así, el puente hacia el estándar tridimensional de justificación judicial propuesto integra tres planos. Las salvaguardas sobre evidencia electrónica aportan criterios para la legitimidad, la epistemología probatoria y los estándares técnicos permiten evaluar la fiabilidad, y el derecho de defensa exige una contradicción efectiva. Definitivamente, ninguno de estos planos sustituye a los demás.

3. Naturaleza procesal del informe OSINT y límites de la ratificación del analista

A los efectos de este estudio, el informe OSINT es el producto documentado mediante el cual se incorporan al proceso los resultados

[28] FERRER BELTRÁN (2007), p. 65 y 151.

de la localización, obtención, preservación, verificación y análisis de información procedente de fuentes abiertas. Su estructura comprende, por tanto, las fuentes utilizadas; el procedimiento de recopilación y preservación; las herramientas empleadas y sus versiones; las operaciones de verificación, transformación o correlación; la cadena inferencial que conecta los datos con la conclusión; las limitaciones del análisis y la identificación de las personas responsables de cada actuación.

Desde una perspectiva procesal penal, el informe constituye un soporte documental, pero esta circunstancia no determina por sí sola su tratamiento como prueba documental. Así, partiendo de la distinción formulada por Freeman, la clasificación probatoria debe atender al objeto incorporado y a las operaciones realizadas sobre la información digital; así, las fotografías, los vídeos, las imágenes aéreas y satelitales, los registros de llamadas y las comunicaciones electrónicas pueden examinarse como documentos. En cambio, cuando el material ha sido sometido a procedimientos forenses o se ha elaborado un producto analítico a partir de datos digitales, como una fotografía geolocalizada o una secuencia de llamadas, su incorporación puede requerir conocimiento experto[29].

Dicho de otro modo, el informe OSINT no constituye un medio de prueba autónomo ni posee una naturaleza procesal única, sino que su encaje dependerá de su contenido y de la función que cumpla en el caso concreto, ya que las fuentes originales pueden tener carácter documental; las operaciones técnicas y las inferencias especializadas, naturaleza pericial; y la declaración del analista, una dimensión testimonial limitada a las actuaciones que hubiera realizado o percibido directamente. Estas dimensiones pueden concurrir, pero no son intercambiables. El presente análisis se circunscribe exclusivamente a la admisión, valoración y eventual exclusión de estos informes dentro del proceso penal.

Con base en lo anterior, la figura del testigo-perito resulta útil para comprender situaciones en las que una persona combina conocimiento directo y técnico. En España, aunque referida a un supuesto ajeno a la prueba digital, la STC 77/2024 ilustra por analogía que la declaración de un funcionario con esa doble aportación (testigo-perito) genera

[29] FREEMAN (2018), p. 296-297.

cuestiones sobre su naturaleza, la inmediación y la contradicción[30]. Aunque esta analogía sirve para delimitar la función del analista, no convierte automáticamente el informe OSINT en testimonio ni permite eludir las garantías de la prueba pericial[31].

La declaración personal ofrece una oportunidad de contradicción, pues el analista puede explicar cuándo accedió a una fuente, cómo la preservó, qué decisiones adoptó y cuáles son las limitaciones del análisis. No obstante, presenta tres límites que conviene diferenciar.

El primero es de carácter conceptual. A diferencia del testigo que conoce los hechos antes y al margen del proceso, el analista suele acceder a ellos como consecuencia de un encargo de investigación. Por ello, su actividad se aproxima a una diligencia técnica o pericial.

El segundo deriva del trabajo colaborativo, pues, conforme describen Gillett & Fan, la DOSI desafía ese paradigma centrado en el individuo. Con frecuencia es recopilada por grupos multidisciplinarios de personas con diversos conocimientos y niveles de experiencia, que trabajan en colaboración: una persona puede recopilar, otra preservar, una tercera configurar la herramienta y una cuarta formular la inferencia. En estos casos, quien firma el documento quizá no esté en condiciones de responder por todas las operaciones, tal como señalan estos autores. La decisión debe, por tanto, identificar responsabilidades y determinar qué especialistas resultan necesarios para contestar las objeciones relevantes[32].

---

[30] ESPAÑA, Tribunal Constitucional, STC 77/2024, de 20 de mayo, ECLI:ES:TC:2024:77. ESPAÑA, Tribunal Constitucional, STC 77/2024, de 20 de mayo, ECLI:ES:TC:2024:77. Esta decisión se enmarca en el artículo 24 de la Constitución española y examina el tratamiento probatorio de la declaración de un inspector de Trabajo en condición de testigo-perito. Cabe resaltar que en España no existe una regulación probatoria específica de los informes OSINT asistidos por IA, por lo que su tratamiento depende de su contenido y función procesal, sino que su admisión se somete a las reglas generales de pertinencia y control de legalidad previstas en los artículos 659 y 785 de la Ley de Enjuiciamiento Criminal. Cuando se limita a recopilar fuentes digitales puede recibir tratamiento documental, mientras que, si incorpora conocimientos especializados o inferencias técnicas, resulta aplicable el régimen pericial de los artículos 456 y 478. Finalmente, su valoración corresponde al tribunal, junto con las demás pruebas practicadas, conforme al artículo 741.

[31] BUENO DE MATA (2023), pp. 256–257.

[32] GILLETT-FAN (2023), p. 680-681.

El tercer límite concierne a la herramienta. El analista puede explicar los datos introducidos y su interpretación, pero desconocer el funcionamiento, el entrenamiento o el margen de error del sistema. La mera supervisión humana no convalida una salida que el propio supervisor no puede comprender críticamente. De ahí que la explicación personal deba apoyarse en registros, documentación técnica y materiales auditables. De lo anterior se sigue que la ratificación no constituye una fórmula de saneamiento. La motivación debe diferenciar la credibilidad del declarante de la fiabilidad del método, precisar qué conocimiento directo posee, qué tareas realizaron terceros y qué elementos externos corroboran su explicación.

4. Un estándar tridimensional de justificación judicial

Conviene precisar el alcance de la propuesta. La valoración permite determinar el grado de corroboración que las pruebas proporcionan a una hipótesis, mientras que el estándar de prueba fija el umbral a partir del cual esta puede considerarse probada[33]. En consecuencia, el estándar tridimensional de justificación judicial aquí formulado no sustituye ese umbral, sino que ordena las razones que deben exteriorizarse cuando el tribunal atribuye eficacia a un informe OSINT asistido por IA .

También debe distinguirse entre la admisión y el peso probatorio. La incorporación de un informe al proceso no determina por sí misma el apoyo que prestará a la hipótesis acusatoria. Como explica Trevisan, en la práctica de la Corte Penal Internacional la mayoría de las pruebas suele admitirse, mientras que las cuestiones relativas a su relevancia, valor probatorio y posible efecto perjudicial se examinan posteriormente, al determinar el peso que corresponde atribuirles[34]. Aunque este modelo no puede trasladarse mecánicamente a los ordenamientos nacionales, permite sostener la necesidad de motivar separadamente la admisión del informe y el peso probatorio que finalmente se le atribuye.

---

[33] FERRER BELTRÁN (2020), p. 377-378.

[34] TREVISAN (2021), p. 7.

La propuesta se articula en tres dimensiones acumulativas, aunque su intensidad varía según las particularidades del caso. Esta estructura se explica porque la obtención lícita no vuelve fiable una inferencia. Del mismo modo, un método técnicamente correcto tampoco permite utilizar el resultado cuando la defensa careció de una oportunidad real para impugnarlo.

A continuación, los aspectos que integran cada dimensión y la finalidad que cumplen dentro de la justificación judicial son representados en el siguiente cuadro. Así, las tres dimensiones son acumulativas, pero no constituyen una secuencia rígida ni una lista de comprobación uniforme. Igualmente, la intensidad de su examen dependerá de la función del informe, de su complejidad técnica, de su peso probatorio y de las objeciones planteadas por las partes. Asimismo, la ausencia o deficiencia de alguno de sus elementos no determina automáticamente una consecuencia procesal, que deberá establecerse conforme al derecho interno aplicable.

Cuadro 1. Contenido del estándar tridimensional de justificación judicial

Dimensión	Aspectos que deben justificarse	Finalidad
Legitimidad	Base normativa, autoridad, finalidad, necesidad, proporcionalidad, alcance, duración y terceros afectados	Determinar la licitud de la obtención y utilización de la información.
Fiabilidad epistémica	Procedencia, autenticidad, integridad, preservación, herramienta, método, limitaciones, inferencia y corroboración	Justificar por qué las fuentes, el procedimiento y las inferencias merecen confianza.

Dimensión	Aspectos que deben justificarse	Finalidad
Contra-dicción efectiva	Acceso a fuentes y registros, responsables, explicación técnica, tiempo y capacidad para impugnar	Comprobar que la defensa pudo conocer, examinar y controvertir eficazmente el informe.

4.1. Legitimidad

En primer lugar, la resolución debe identificar la base jurídica de la actuación y el sujeto habilitado para realizarla. En particular, no merece la misma respuesta una observación puntual que un monitoreo prolongado, el uso de una identidad encubierta o una orden dirigida a un proveedor. La etiqueta OSINT no puede ocultar el nivel real de injerencia.

La finalidad concreta de la recopilación y su relación con una investigación constituyen un segundo elemento que debe exponerse. Las búsquedas generales destinadas a detectar conductas potencialmente ilícitas presentan un riesgo mayor de vigilancia indiscriminada. Por ello, cuando la selección depende de palabras clave, categorías o perfiles de riesgo, la decisión ha de examinar su pertinencia y la posibilidad de que produzcan falsos positivos.

También el momento de la recopilación modifica este análisis. Si precedió a la noticia criminal, deben explicarse la habilitación preventiva y las salvaguardas frente a una exploración indiscriminada. Si se produjo dentro de una investigación formalizada, corresponde comprobar su conexión con el objeto, las personas y los límites autorizados.

Por último, el control retrospectivo de proporcionalidad debe considerar la idoneidad, la necesidad, la duración, el volumen, las categorías de datos y la afectación de terceros. Si existió una autorización previa, la decisión comprobará que la ejecución no excedió sus términos. Si el control fue posterior, deberá evitar que la utilidad del resultado justifique retrospectivamente una intervención que carecía de razones suficientes.

4.2. Fiabilidad epistémica

En esta segunda dimensión, la resolución debe examinar la fiabilidad del recorrido probatorio. Ello comprende la autenticidad e integridad de los materiales, la ausencia de manipulaciones relevantes y la solidez del método y de las inferencias que conectan las fuentes con la conclusión[35]. Así, ha de identificar la fuente, explicar cómo se atribuyó a una persona o entidad y señalar qué elementos permiten excluir una suplantación. En particular, un nombre y una fotografía no demuestran por sí solos quién administra una cuenta. La atribución puede requerir metadatos, coincidencias temporales, enlaces con otras cuentas o información adicional.

Cabe puntualizar que la autenticidad y la integridad deben analizarse por separado, tal como apunta White, para quien la primera examina la correspondencia del material con su origen alegado, mientras que la segunda permite determinar si este se mantuvo sin alteraciones relevantes[36]. La autenticidad tradicionalmente ha recaído en la verificación de la cadena de custodia, empero, aunque el *hash* realmente solo constituye un dato útil respecto de la integridad y ni siquiera en este aspecto aporta una garantía absoluta.

Cuando intervenga IA, el tribunal debe identificar su función concreta y, cuando sea relevante, la versión del sistema. Para ello, debe conocer si la herramienta localizó fuentes, clasificó resultados, reconoció elementos, estableció coincidencias o produjo una conclusión. La motivación deberá considerar las limitaciones conocidas, la calidad de los datos, la posibilidad de falsos positivos y la supervisión humana.

Además, el método ha de ser suficientemente auditable. La volatilidad de las fuentes puede impedir una reproducción idéntica, pero un especialista debe poder reconstruir el proceso mediante las consultas, los criterios de selección, los registros y las transformaciones documentadas. Las operaciones manuales también requieren explicación, pues los sesgos pueden introducirse antes o después de la automatización.

---

[35] GONZÁLEZ REYES (2021), p. 50.

[36] WHITE (2024), p. 232.

El análisis culmina con el control de la cadena de inferencia. La decisión ha de identificar los hechos básicos, las generalizaciones que los conectan con la conclusión y las hipótesis alternativas plausibles. Cuanto más decisiva sea la atribución personal, mayor será la necesidad de corroboración independiente. Así, la coincidencia entre fuentes que derivan del mismo origen no constituye una corroboración real.

Ello no obliga a descartar cualquier hipótesis imaginable. Sin embargo, cuando el informe sea determinante para una condena, sí deberán contestarse las alternativas compatibles con la inocencia que hayan sido concretamente planteadas, como la suplantación, la gestión compartida de una cuenta, la homonimia, la manipulación o el error de correlación.

4.3. Contradicción efectiva

La tercera dimensión se refiere a las condiciones en las que el informe fue revelado, explicado y debatido. Aunque el juez no dirige la estrategia defensiva, debe justificar que la prueba relevante fue efectivamente accesible y susceptible de contradicción. Desde esta perspectiva, la mera entrega de una conclusión o visualización resulta insuficiente si las fuentes, las consultas y los registros permanecen inaccesibles. Como advierte Sampson, la defensa debe conocer qué información fue incluida, qué elementos se descartaron y qué operaciones condujeron al resultado[37].

También deben individualizarse los responsables de recopilar, preservar, configurar la herramienta y formular la inferencia. No siempre será indispensable que todos ellos comparezcan, pero la decisión deberá explicar por qué la prueba personal ofrecida permite responder a las objeciones planteadas.

Las herramientas propietarias generan una tensión adicional. El secreto comercial, sin embargo, no puede eliminar la posibilidad de impugnar una prueba decisiva. Pueden adoptarse medidas de acceso restringido, disponer la intervención de expertos independientes o exigir la entrega de documentación equivalente. Si ninguna alternativa permite

[37] SAMPSON (2016), p. 300.

conocer los aspectos esenciales del método, la opacidad deberá reflejarse en el peso atribuido al resultado o, en los supuestos más graves, impedir su utilización.

A ello se añaden el tiempo y la capacidad técnica necesarios para ejercer la contradicción. La entrega tardía de grandes volúmenes de información o de registros incomprensibles no satisface el derecho de defensa. Según las particularidades del caso, será necesario facilitar formatos adecuados, permitir un contraanálisis y conceder acceso a especialistas. La resolución debe responder de manera individualizada a las objeciones concretas.

5. Defectos y consecuencias procesales

Las categorías de subsanación, corroboración, reducción del peso probatorio, inadmisión, exclusión y nulidad se presentan como posibles respuestas, no como instituciones equivalentes ni como soluciones uniformemente aplicables, cuyo significado y procedencia dependen del derecho interno. Sin perjuicio de ello, para graduar la respuesta, conviene distinguir entre los defectos de licitud, los fallos de autenticidad o integridad, las limitaciones metodológicas y las restricciones de contradicción. La solución dependerá de la gravedad del defecto, del carácter decisivo del informe y de su posibilidad de reparación.

Un primer nivel comprende las deficiencias documentales subsanables. Así, la omisión inicial de la versión de una herramienta o del registro de una operación puede corregirse mediante la documentación correspondiente o la comparecencia de la persona responsable. Como pauta de justificación, y siempre que el ordenamiento aplicable lo permita, la deficiencia debería aclararse antes de atribuir pleno valor al informe.

Un segundo nivel incluye las limitaciones que no destruyen la fiabilidad, pero impiden tratar el resultado como autosuficiente. Esto puede ocurrir cuando una captura fue preservada de forma incompleta, aunque su contenido coincida con fuentes independientes, o cuando se conoce un margen de error. La respuesta puede consistir en exigir una corroboración adicional y reducir el peso probatorio.

El tercer nivel aparece cuando la opacidad impide reconstruir una inferencia decisiva. Si se desconocen las fuentes, la herramienta no puede ser examinada o el analista no explica el paso desde los datos hasta la conclusión, el tribunal carece de razones suficientes para otorgarle fuerza incriminatoria autónoma. Por tanto, la inferencia deberá excluirse del razonamiento o utilizarse únicamente con un alcance orientativo.

El cuarto y último nivel comprende las vulneraciones de derechos fundamentales o las quiebras irreparables de autenticidad y contradicción. Una medida sin base jurídica, el acceso a datos protegidos fuera de los límites autorizados o la imposibilidad de determinar si el material fue alterado pueden justificar la inadmisión, la exclusión o la nulidad conforme al derecho interno. Esta consecuencia no deriva automáticamente de los artículos 15 o 24, aunque sus salvaguardas ayudan a apreciar la gravedad de la afectación.

Una decisión argentina sobre la nulidad de una pericia digital muestra la utilidad de esta graduación. La falta de notificación a la defensa, la ausencia de documentación técnica y la modificación de archivos durante la custodia impidieron asegurar que el material analizado coincidiera con el original. La nulidad no respondió a una omisión meramente ritual, sino a la acumulación de defectos que afectaron la integridad, la reproducibilidad y la defensa[38].

En cambio, la jurisprudencia española rechaza que cualquier irregularidad en la cadena de custodia determine automáticamente la inutilización. Exige valorar si existen garantías suficientes de autenticidad y si la objeción identifica un riesgo concreto de manipulación. Esta aproximación evita el formalismo, pero obliga a explicar por qué otros

[38] ARGENTINA, Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, Sala I, Fiscal s/apela declaración de nulidad de informe pericial, causa n. 46.744, registro n. 458, 24 mayo 2012. Tal resolución aplicó los artículos 200, 201 y 258 del Código Procesal Penal de la Nación, disposiciones que exigen notificar a la defensa antes de practicar pericias definitivas o irreproducibles y, en particular, antes del inicio de las operaciones periciales, bajo pena de nulidad. Esta decisión se cita únicamente para ilustrar las consecuencias previstas por ese régimen procesal y no como una solución extrapolable a otros ordenamientos.

elementos compensan el defecto. La invocación genérica de la libre valoración no constituye una respuesta suficiente[39].

La motivación insuficiente puede producir errores de diferentes maneras. Puede conceder una autoridad excesiva a una salida automatizada, confundir correlación con identificación, ignorar hipótesis alternativas o utilizar como corroboración datos dependientes de una misma fuente. A ello se suma el riesgo de trasladar indebidamente a la defensa la carga de probar una manipulación cuando la acusación no ha acreditado previamente la procedencia y el método.

Conviene aclarar que la intensidad de la motivación debe ser proporcional al peso del informe, a la complejidad del sistema y a la entidad de las objeciones planteadas. Así, un elemento periférico y corroborado requiere un desarrollo menor que una atribución automatizada decisiva para establecer la autoría, siguiendo un razonamiento análogo al que exige un carácter reforzado de la motivación cuando se impone una condena, en contraste con los casos de absolución[40]. Además, si bien todo proceso conlleva en sí mismo una complejidad e incertidumbre inherentes a las situaciones procesales[41], esta se eleva cuando el uso de una tecnología amplifica la asimetría informativa y el riesgo de error, lo que exige reforzar los mecanismos de control.

Conclusiones

Primera. OSINT no constituye un medio de prueba autónomo. Por ello, la decisión debe diferenciar la fuente digital, su recopilación,

---

[39] ESPAÑA, Tribunal Supremo, Sala de lo Penal, STS 1170/2024, de 19 de diciembre, ECLI:ES:TS:2024:6259; STS 116/2025, de 13 de febrero, ECLI:ES:TS:2025:634. Ambas resoluciones examinan las objeciones relativas a la autenticidad, integridad y cadena de custodia dentro del marco del artículo 24.2 de la Constitución y de las reglas de valoración y revisión previstas en la Ley de Enjuiciamiento Criminal, especialmente sus artículos 741, 849.2 y 852. Su doctrina no atribuye a cualquier irregularidad un efecto automático de exclusión, sino que exige valorar su incidencia concreta sobre la autenticidad, la integridad y el derecho de defensa.

[40] BELTRÁN CALFURRAPA (2024), p. 24.

[41] VASCONCELLOS (2018), p. 714.

preservación, transformación analítica, el informe y la declaración de quien intervino. Esta separación permite localizar el defecto y evita que la autenticidad de un archivo se confunda con la verdad de su contenido o con la corrección de la inferencia.

Segunda. El carácter públicamente accesible de una fuente no elimina el examen jurídico. En particular, la escala, la duración, la agregación, la automatización, las barreras de acceso, la finalidad y la afectación de terceros pueden transformar una observación puntual en una actuación estatal intensiva. La etiqueta OSINT no determina, por sí sola, el régimen aplicable.

Tercera. El artículo 15 del Convenio de Budapest y el artículo 24 de la Convención de las Naciones Unidas aportan criterios relevantes de legalidad, proporcionalidad, control y recurso efectivo, pero no regulan la valoración de los informes OSINT. Su función se concentra en la dimensión de legitimidad. Por tanto, la fiabilidad y la contradicción requieren fundamentos adicionales en la epistemología probatoria, los estándares técnicos y el proceso justo.

Cuarta. La ratificación personal del analista no convalida el informe. En las investigaciones colaborativas y automatizadas, quien comparece puede desconocer las operaciones realizadas por terceros o por la herramienta. De ahí que la motivación deba distinguir entre la credibilidad personal y la fiabilidad metodológica, individualizar responsabilidades y asegurar una documentación auditable.

Quinta. Una decisión suficientemente motivada debe responder a tres dimensiones interrelacionadas. En la legitimidad explicará la base jurídica, la autoridad, la finalidad, la necesidad, la proporcionalidad, el alcance y la afectación de terceros. En la fiabilidad justificará la procedencia, la autenticidad, la integridad, la preservación, la función de la IA, el método, las inferencias y la corroboración. En cuanto a la contradicción, comprobará el acceso, la explicación, el tiempo y la capacidad efectiva de impugnación.

Sexta. Los defectos exigen una respuesta graduada. Las omisiones reparables permiten su subsanación. Las limitaciones que reducen, sin destruir, la confianza requiere corroboración y justifican la atribución de un menor peso probatorio. La imposibilidad de reconstruir una inferencia impide atribuirle fuerza autónoma. Por último, las vulneraciones graves

o irreparables pueden conducir a la inadmisión, la exclusión o la nulidad conforme al derecho interno.

A la luz de las conclusiones anteriores, la respuesta a la pregunta que guía esta investigación es que una decisión judicial sobre la admisión, valoración o exclusión de un informe OSINT asistido por IA no queda suficientemente justificada mediante la mera ratificación del analista o la invocación genérica de protocolos técnicos. La decisión debe exteriorizar razones referidas, de manera interrelacionada, a la legitimidad de la obtención y utilización de la información, la fiabilidad epistémica de la cadena inferencial y la posibilidad efectiva de contradicción. En definitiva, el estándar propuesto no privilegia ni desconfía de la tecnología por sí misma, sino de someter su utilización probatoria a razones justificadas, comprensibles y susceptibles de contradicción.

Referencias

BELTRÁN CALFURRAPA, Ramón. Los vicios de la motivación como causa del error judicial: un primer esbozo. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 10, n. 2, p. 1-38, 2024. https://doi.org/10.22197/rbdpp.v10i2.924

BUENO DE MATA, Federico. *Investigación y prueba de delitos de odio en redes sociales: técnicas OSINT e inteligencia policial*. Valencia: Tirant lo Blanch, 2023.

CENTRO DE ESTUDIOS LEGALES Y SOCIALES (CELS). La justicia federal sobreseyó a Kevin Guerra por sus expresiones en Twitter. Disponible en: https://www.cels.org.ar/web/2021/01/la-justicia-federal-sobreseyo-a-kevin-guerra-por-sus-expresiones-en-twitter/ Acceso en: 12 set. 2026.

FERRER BELTRÁN, Jordi. *La valoración racional de la prueba*. Madrid: Marcial Pons, 2007.

FERRER BELTRÁN, Jordi. Sobre el deber de motivación de las decisiones probatorias y el juicio por jurados. La sentencia V.R.P., V.P.C. y otros vs. Nicaragua de la Corte IDH. *Quaestio Facti. Revista Internacional sobre Razonamiento Probatorio*, n. 1, p. 359-382, 2020. https://doi.org/10.33115/udg_bib/qf.i0.22381

FISBERG, Yuri. Função 'hash' e a integridade da prova digital. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 11, n. 3, p. 1-45, 2025. https://doi.org/10.22197/rbdpp.v11i3.1227

FREEMAN, Lindsay. Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials. *Fordham International Law Journal*, vol. 41, n. 2, p. 283-336, 2018. https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1

GHIONI, Riccardo; TADDEO, Mariarosaria; FLORIDI, Luciano. Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*, vol. 39, n. 4, p. 1827-1842, 2024. https://doi.org/10.1007/s00146-023-01628-x

GILLETT, Matthew; FAN, Wallace. Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom. *Journal of International Criminal Justice*, vol. 21, n. 4, p. 661-693, 2023. https://doi.org/10.1093/jicj/mqad050

GONZÁLEZ REYES, José Miguel. La prueba pericial digital y la cadena de custodia. *Anales de la Facultad de Derecho*, n. 38, p. 43-79, 2021. https://doi.org/10.25145/j.anfade.2021.38.03

JAMARDO LORENZO, Andrea. La dimensión tecnológica de la cadena de custodia: algunas claves. *InDret*, n. 2, pp. 298-345, 2025. https://doi.org/10.31009/InDret.2025.i2.07

MOLINA, Pablo Antonio. El uso de la inteligencia artificial en el proceso penal: una mirada a la luz del deber de motivación y de la averiguación de la verdad sobre los hechos del caso. En: LEZCANO, José María; IUALE, Corina; LICEDA, Ernesto (org.). *Encuentro Derecho y Tecnología 2020*. La Plata: Universidad Nacional de La Plata, 2022, p. 142-148. Disponible en: https://libros.unlp.edu.ar/index.php/unlp/catalog/book/2131 Acceso en: 30 jul. 2026.

OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS; HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY. *Berkeley Protocol on Digital Open Source Investigations*. Disponible en: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf Acceso en: 30 jul. 2026.

RAGHAVAN, Sriram. Digital forensic research: current state of the art. *CSI Transactions on ICT*, vol. 1, n. 1, p. 91-114, 2013. https://doi.org/10.1007/s40012-012-0008-7

SAMPSON, Fraser. Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings. En: AKHGAR, Babak; BAYERL, P. Saskia; SAMPSON, Fraser (org.). *Open Source Intelligence Investigation: From Strategy to Implementation*. Cham: Springer, 2016, p. 295-304. https://doi.org/10.1007/978-3-319-47671-1_18

TREVISAN, Stefano. Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol. *Giurisprudenza Penale Web*, n. 4, p. 1-17, 2021. Disponible en: https://www.giurisprudenzapenale.com/wp-content/uploads/2021/04/Trevisan_gp_2021_4.pdf Acceso en: 30 jul. 2026.

VASCONCELLOS, Vinicius Gomes. A prova no processo penal: a importância da valoração do lastro probatório e de seu controle por meio recursal. *Revista Eletrônica do Curso de Direito da UFSM*, vol. 13, n. 2, p. 695-721, 2018. https://doi.org/10.5902/1981369430012

WHITE, Elizabeth. Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism. *Leiden Journal of International Law*, vol. 37, n. 1, p. 228-250, 2024. https://doi.org/10.1017/S0922156523000444

BACHMAIER WINTER, Lorena. A luta pelas garantias processuais e a mudança de paradigma em matéria de prova: do liberalismo à mass surveillance no processo penal europeu. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 11, n. 1, p. 1-56, 2025. https://doi.org/10.22197/rbdpp.v11i1.1164

Authorship information

Wendy Requejo Passoni. Máster en Derecho Penal por la Universidad de Salamanca y Máster en Ciberseguridad y Entornos Digitales por la Universidad de León. Doctora en Derecho con mención internacional por la Universidad de Salamanca. Vinculada académicamente a la Universidad Científica del Sur, Lima, Perú. Sus líneas de investigación comprenden el Derecho Penal, Derecho de la Ciberseguridad, Ciberdelincuencia, Prueba digital y las nuevas tecnologías. Correo electrónico: wrequejo@cientifica.edu.pe

Additional information and author's declarations
(*scientific integrity*)

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

Declaration of originality: the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

Data Availability Statement: In compliance with open science policies, all data generated or analyzed during this study are included in this published article.

IA Statement: The authors declare that they are aware that the use of artificial intelligence must not supplant the human originality of the research, and that full responsibility for any errors or plagiarism rests entirely with the authors. The author declare that IA was used in the following stages of this research: drafting, language editing, and formatting the bibliography in accordance with the journal's guidelines.

Editorial process dates (https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 30/07/2026
- Desk review and plagiarism check: 31/07/2026
- Review 1: 25/08/2026
- Review 2: 25/08/2026
- Preliminary editorial decision: 05/09/2026
- Correction round return: 20/09/2026
- Final editorial decision: 21/09/2026

Editorial team

- Editor-in-chief: 1 (VGV)
- Associated-editor: 2 (RB; FC)
- Reviewers: 2

How to cite (ABNT Brazil):

REQUEJO-PASSONI, Wendy. Inteligencia de fuentes abiertas (OSINT) y motivación judicial: un estándar tridimensional para la prueba penal. *Revista Brasileira de Direito Processual Penal*, vol. 12, n. 3, e1619, set./dez. 2026. https://doi.org/10.22197/rbdpp.v12i3.1619



License Creative Commons Attribution 4.0 International.