

EL PERFIL QUE NO ESCRIBISTE: IDENTIDAD DIGITAL, BIOMETRÍA OCULAR Y AUTORIDAD SEMÁNTICA EN SISTEMAS ALGORÍTMICOS PREDICTIVOS

*The Profile You Didn't Write: Digital Identity, Ocular Biometrics and
Semantic Authority in Predictive Algorithmic Systems*

Carlos Eduardo Ravello Joo
ORCID: 0009-0007-5631-7436

carlosravello.com

Trujillo — Lima, Perú

Mayo 2026

Nota del autor

Este trabajo es el segundo de una serie de preprints independientes depositados en Zenodo. El primero — Ravello Joo (2026) — estableció el marco conceptual de la Metacognición 2.0 y el Modelo de Coherencia Dinámica (MCD). Este documento extiende ese marco hacia el dominio de la biometría ocular y la vigilancia algorítmica como contexto que hace operativamente necesaria la capacidad propuesta. No ha recibido financiamiento externo. El autor declara ausencia de conflicto de intereses.

RESUMEN

Este trabajo examina la arquitectura de vigilancia algorítmica contemporánea desde la perspectiva del agente individual que opera en entornos digitales de alta visibilidad. Se argumenta que la identidad digital de un individuo no es únicamente el resultado de sus declaraciones explícitas — es fundamentalmente una construcción inferida por sistemas predictivos a partir de rastros de comportamiento no autorizados deliberadamente. La evidencia documentada muestra que plataformas de fitness, redes profesionales y aplicaciones de salud generan, agregan y comercializan señales de comportamiento individual con terceros (Federal Trade Commission, 2014; Reviglio, 2022), y que estos datos son utilizados para construir perfiles psicográficos con consecuencias laborales, financieras y asegurativas medibles (Schneble et al., 2018; Wilcox et al., 2021). El trabajo introduce además una dimensión emergente y subestimada en la literatura: la biometría ocular — reconocimiento de iris, scleral pattern recognition y gaze tracking — como nueva frontera de captura de identidad con características únicas de permanencia e irrevocabilidad (Bhatt et al., 2025; Doke et al., 2024). Se propone que estos desarrollos hacen operativamente necesaria la capacidad descrita en el trabajo anterior del autor como Metacognición 2.0 (Ravello Joo, 2026): la habilidad de modelar deliberadamente cómo los sistemas de inteligencia artificial procesan una identidad, y de diseñar esa identidad para que el output clasificatorio sea el que el agente decidió. Se presenta el Modelo de Coherencia Dinámica (MCD) como respuesta estructural a esta asimetría de información.

Palabras clave: identidad digital, biometría ocular, vigilancia algorítmica, autoridad semántica, knowledge graph, reconocimiento de iris, gaze tracking, data brokers, Metacognición 2.0, Modelo de Coherencia Dinámica

1. INTRODUCCIÓN

Este artículo constituye una propuesta de marco conceptual basada en la experiencia profesional documentada del autor y en revisión narrativa crítica de literatura académica verificable. No es un estudio empírico formal.

La mayoría de los individuos que operan en entornos digitales asume, de forma implícita, que su identidad digital es el resultado de lo que han publicado, declarado o compartido de forma consciente. Esa asunción es incorrecta.

Los sistemas algorítmicos contemporáneos no esperan la declaración del agente. Infieren. Clasifican. Construyen modelos predictivos sobre él a partir de señales que el agente, frecuentemente, no sabe que está produciendo. El rastro de breadcrumbs digitales — búsquedas, likes, patrones de actividad física, rutas de desplazamiento, frecuencia cardíaca, microexpresiones faciales en una entrevista de trabajo automatizada, la dirección de la mirada dentro de un visor de realidad aumentada — constituye un conjunto de datos de comportamiento que los sistemas procesan con precisión creciente y consecuencias reales.

El trabajo anterior del autor (Ravello Joo, 2026) estableció el marco conceptual para responder a esta realidad: la Metacognición 2.0, definida como la capacidad de modelar deliberadamente cómo los sistemas de inteligencia artificial procesan una identidad digital, y el Modelo de Coherencia Dinámica (MCD) como herramienta operativa para implementar esa capacidad. Este trabajo extiende ese marco en dos direcciones. Primero, documenta con mayor profundidad el paisaje de vigilancia algorítmica que hace necesaria esa capacidad — con énfasis en la comercialización de datos de comportamiento y el uso de perfiles psicográficos inferidos. Segundo, introduce una dimensión que el trabajo anterior no abordó: la biometría ocular como frontera emergente de captura de identidad con características radicalmente distintas a cualquier dato digital previo. Un iris no se puede cambiar. Un patrón de venas esclerales no se puede borrar. Eso transforma la naturaleza del problema.

2. MARCO TEÓRICO

2.1 Grafos de conocimiento, PageRank y propagación de autoridad semántica

Los sistemas de búsqueda modernos organizan el conocimiento sobre entidades — personas, organizaciones, conceptos — mediante grafos de conocimiento: estructuras de datos donde los nodos representan entidades y las aristas representan relaciones entre ellas. La autoridad de un nodo en ese grafo no es una propiedad intrínseca — es una función de las relaciones que mantiene con otros nodos.

El algoritmo PageRank, formalizado por Brin y Page (1998), establece que la autoridad de un nodo A se calcula como:

$$PR(A) = (1-d) + d \times \sum PR(T)/C(T)$$

Donde d es el factor de amortiguación (convencionalmente 0.85), T son los nodos que apuntan a A , y $C(T)$ es el número de enlaces salientes de cada nodo T . La implicación operativa es directa: la autoridad de una entidad en el grafo depende de la autoridad de las entidades con las que está conectada. Una entidad conectada a nodos de baja autoridad o reputación comprometida ve su propio valor de autoridad descender proporcionalmente — no como consecuencia moral sino como operación matemática.

Kejriwal (2023) documentó que en grafos de conocimiento personales — los que organizan información sobre individuos — la resolución de entidades depende críticamente de la coherencia entre señales provenientes de fuentes independientes, y que la ausencia de esa coherencia produce clasificaciones fragmentadas o de baja autoridad. Hu et al. (2025) extendieron ese análisis hacia sistemas de resolución de entidades basados en redes neuronales en grafos de propiedades, documentando que la propagación de atributos entre nodos adyacentes opera de forma automática e independiente de la intención del agente.

2.2 Embeddings de grafos y reposicionamiento vectorial de identidad

Los sistemas modernos de procesamiento de grafos van más allá del PageRank estático. Grover y Leskovec (2016) formalizaron Node2Vec como framework para el aprendizaje de representaciones de nodos que preserva la estructura de vecindarios: cada nodo del grafo se convierte en un vector numérico en un espacio de alta dimensionalidad, donde la proximidad entre vectores refleja la similitud semántica entre nodos. Wang et al. (2021) extendieron ese enfoque hacia grafos de conocimiento mediante KG2Vec, documentando que las relaciones semánticas entre entidades se preservan en el espacio vectorial resultante.

La consecuencia para la identidad digital es que una asociación entre nodos — una foto en una fiesta, una aparición junto a una entidad de reputación comprometida, una interacción en una plataforma de redes sociales — no produce un efecto meramente reputacional en el sentido humano del término. Produce una reposición matemática del nodo afectado en el espacio vectorial. Esa reposición tiene consecuencias medibles en los sistemas de clasificación que operan sobre ese espacio.

2.3 Biometría ocular: iris, sclera y gaze tracking

La biometría ocular representa una categoría cualitativamente distinta de los datos de comportamiento digital descritos hasta ahora. Mientras que una

contraseña filtrada puede cambiarse, un número de teléfono puede modificarse y un patrón de actividad en redes sociales puede alterarse mediante esfuerzo deliberado, el iris y el patrón de venas esclerales son características anatómicas permanentes e irrevocables.

Bhatt et al. (2025) documentaron en una revisión sistemática que el reconocimiento de iris ha alcanzado niveles de precisión que lo posicionan como uno de los identificadores biométricos más confiables disponibles, con aplicaciones que van desde identificación forense hasta control de acceso en instalaciones de alta seguridad. Anne et al. (2019) evaluaron la factibilidad y aceptabilidad de sistemas de reconocimiento de iris para identificación única de pacientes en entornos reales de servicios de salud en Kenya, documentando tanto su efectividad técnica como las tensiones éticas que su implementación genera en poblaciones con acceso limitado a información sobre sus derechos.

Doke et al. (2024) documentaron el scleral pattern recognition — el reconocimiento del patrón de venas del ojo blanco — como modalidad biométrica emergente con propiedades de unicidad superiores al iris mismo, más difícil de falsificar y más resistente a las condiciones ambientales que afectan el reconocimiento de iris convencional. Crihalmeanu y Ross (2012) establecieron las bases técnicas del reconocimiento multispectral de patrones esclerales, documentando su viabilidad como sistema de identificación robusto.

El gaze tracking — el rastreo de la dirección e intensidad de la mirada — añade una dimensión comportamental a la biométrica. Rodrigues et al. (2026) desarrollaron un framework que integra eye tracking, aprendizaje automático y reconocimiento facial para inferir comportamiento del consumidor con una precisión que supera los métodos de encuesta tradicionales. Lo que el individuo mira, durante cuánto tiempo y con qué intensidad es dato de comportamiento tan informativo como lo que busca en un motor de búsqueda — y en algunos contextos más, porque no está mediado por la racionalización consciente del agente.

2.4 Emotion recognition y evaluación algorítmica de personas

Los sistemas de reconocimiento de emociones extienden la captura biométrica hacia el dominio de los estados internos inferidos. Kulke et al. (2020) compararon el software de análisis de expresiones faciales de Affective con mediciones electromiográficas directas de expresiones faciales,

documentando su capacidad de inferir estados emocionales a partir de video con precisión comparable a la medición fisiológica directa.

HireVue — plataforma de entrevistas automatizadas utilizada por cientos de empresas Fortune 500 — analiza las microexpresiones faciales, el tono de voz y el contenido lingüístico de los candidatos durante entrevistas en video, generando un score de empleabilidad antes de que un evaluador humano revise la candidatura. Ajunwa (2022) criticó este tipo de sistemas comparándolos con la frenología — la pseudociencia del siglo XIX que pretendía inferir capacidades mentales a partir de características físicas — argumentando que la validez predictiva de estos sistemas no está adecuadamente establecida y que sus sesgos algorítmicos reproducen y amplían discriminaciones preexistentes. Kammerer (2022) analizó las implicaciones legales de estas plataformas desde la perspectiva del derecho laboral y la privacidad, documentando las tensiones entre su adopción corporativa y los marcos regulatorios vigentes.

3. REVISIÓN DE LITERATURA Y CASOS DE ESTUDIO

3.1 La comercialización del comportamiento: data brokers y perfiles psicográficos

La Federal Trade Commission documentó en 2014 que doce aplicaciones de salud y fitness compartieron datos de comportamiento de sus usuarios con setenta y seis terceros distintos, incluyendo geolocalización, frecuencia cardíaca y patrones de actividad física. Esa práctica no ha disminuido — se ha normalizado e industrializado.

Reviglio (2022) analizó el rol de los data brokers en la economía de la vigilancia, documentando que operan como intermediarios que agregan datos de comportamiento provenientes de múltiples fuentes, construyen perfiles de individuos y los comercializan a empleadores, aseguradoras, instituciones financieras y organismos gubernamentales. Crain (2018) documentó los límites de la transparencia en ese mercado, argumentando que la opacidad estructural de los data brokers es una característica funcional del sistema, no una deficiencia regulatoria accidental.

Cambridge Analytica construyó perfiles psicográficos de aproximadamente 87 millones de usuarios de Facebook a partir de datos obtenidos mediante una aplicación de test de personalidad instalada voluntariamente por aproximadamente 270,000 usuarios — cuyos permisos de la época permitían el acceso a los datos de todos sus contactos. Schneble et al. (2018) analizaron el caso desde la perspectiva de la ética de la investigación mediada por Internet, documentando las tensiones entre los marcos de consentimiento existentes y las capacidades de extracción de datos que las plataformas sociales permitían. Hu (2020) examinó la opacidad algorítmica del sistema de Cambridge Analytica, argumentando que su capacidad predictiva sobre comportamiento electoral era técnicamente plausible dado el volumen y la granularidad de los datos disponibles.

3.2 Biometría ocular en despliegue: casos documentados

Worldcoin — rebautizada World en 2024, fundada por Sam Altman — operó un sistema de registro biométrico basado en escaneo de iris en múltiples países en desarrollo, incluyendo Perú, Kenya, India e Indonesia, ofreciendo criptomonedas como compensación por el registro. Calungsod (2025) evaluó las implicaciones de privacidad y seguridad del sistema biométrico de World App, documentando las tensiones entre el modelo de negocio de la plataforma y los derechos de los usuarios que cedieron datos biométricos

irrevocables en contextos de información asimétrica.

Los aeropuertos de Dubai y Heathrow operan sistemas de reconocimiento de iris como componente de sus procesos de control de acceso e identificación de viajeros. Meta tiene patentes registradas para sistemas de gaze tracking dentro de sus dispositivos de realidad aumentada Quest, con el propósito declarado de mejorar la experiencia de usuario — y el propósito no declarado de generar datos de comportamiento visual de alta granularidad.

3.3 Behavioral scoring: seguros, empleo y crédito

John Hancock, aseguradora de vida, ofrece pólizas cuya prima se ajusta dinámicamente según los datos de actividad física registrados por dispositivos wearable del asegurado. LinkedIn opera Talent Insights, un producto comercial que genera señales de "flight risk" — riesgo de que un empleado abandone la organización — a partir de su patrón de actividad dentro de la plataforma, y lo comercializa a empleadores. Shaw et al. (2022) documentaron en *Psychological Science* que los rastros digitales individuales presentan consistencia intraindividual estable suficiente para inferir rasgos de personalidad y predecir comportamiento futuro. Wilcox et al. (2021) confirmaron que el escrutinio de huella digital se ha incorporado de forma rutinaria en los procesos de selección de personal, con prevalencia superior al sesenta por ciento en empresas medianas y grandes.

4. DISCUSIÓN

4.1 La asimetría biométrica como problema irreversible

Los datos de comportamiento digital descritos en el trabajo anterior (Ravello Joo, 2026) comparten una característica que los hace manejables en principio: son modificables. Un patrón de actividad en redes sociales puede alterarse. Una huella de búsqueda puede redirigirse. Un historial de interacciones puede reorientarse mediante esfuerzo deliberado y sostenido.

El iris no comparte esa característica. El patrón de venas esclerales tampoco. Eso transforma cualitativamente la naturaleza del problema. Cuando Worldcoin escaneó el iris de individuos en Kenya y Perú a cambio de una compensación monetaria modesta, no capturó un dato que esos individuos pudieran modificar si posteriormente decidieran que la cesión fue un error. Capturó una característica anatómica permanente e irrevocable — y la incorporó a un sistema cuyo uso futuro los cedentes no controlan.

Eso introduce una dimensión ética y operativa que la literatura sobre privacidad digital generalmente no aborda con la especificidad que el problema requiere: la diferencia entre datos que pueden revocarse y datos que no pueden revocarse nunca. Una contraseña filtrada se cambia. Una dirección de correo comprometida se abandona. Un iris escaneado sin consentimiento informado genuino es una cesión permanente sin posibilidad de retractación.

4.2 La propagación de autoridad como mecanismo de contagio

El marco de grafos de conocimiento establece que la autoridad semántica de un nodo depende de las entidades con las que está conectado (Brin & Page, 1998; Grover & Leskovec, 2016). Lo que la literatura técnica describe en términos de optimización matemática tiene consecuencias humanas concretas: la asociación con entidades de reputación comprometida — en fotografías, en menciones, en interacciones en redes sociales — produce una reposición vectorial del nodo afectado con efectos medibles en los sistemas de clasificación que operan sobre ese grafo.

Ese mecanismo opera de forma automática, sin intervención humana, a velocidades que superan la capacidad del agente de detectar y responder al daño. Google crawlea Meta directamente desde 2025, lo que significa que el intervalo entre la producción de una asociación comprometedora y su incorporación al grafo de conocimiento es de horas, no de días o semanas.

Construir coherencia semántica verificable tarda semanas. Degradarla por asociación puede tomar una sola crawleada.

4.3 La Metacognición 2.0 como respuesta estructural

El trabajo anterior (Ravello Joo, 2026) propuso la Metacognición 2.0 como la capacidad de modelar deliberadamente cómo los sistemas de inteligencia artificial procesan una identidad digital. El paisaje documentado en este trabajo hace esa capacidad no solo deseable sino operativamente necesaria para cualquier agente que opere en entornos de alta visibilidad algorítmica.

El Modelo de Coherencia Dinámica (MCD), formalizado mediante el pseudo-ratio:

$$\Omega = V/(M+I)$$

proporciona el marco operativo para implementar esa capacidad. En el contexto de la biometría ocular, los parámetros del modelo adquieren una dimensión adicional: V incluye no solo las señales digitales declaradas sino las biométricas que el agente cede en cualquier interacción con sistemas de reconocimiento; M debe considerar la restricción activa de la exposición biométrica en contextos donde esa exposición no es necesaria; I incorpora la incertidumbre sobre los usos futuros de los datos biométricos ya cedidos.

El atractor natural del sistema en $\Omega \approx 0.66$ (Ravello Joo, 2026) sigue siendo operativamente válido — pero la naturaleza irrevocable de los datos biométricos modifica la función de costo del error: subestimar M en el dominio biométrico produce un costo permanente que no puede corregirse mediante ajuste posterior del sistema.

4.4 Implicaciones regulatorias

El GDPR europeo clasifica los datos biométricos como categoría especial de datos personales que requiere base legal reforzada para su procesamiento. La Illinois Biometric Information Privacy Act (BIPA) establece en Estados Unidos que las entidades que capturan datos biométricos deben obtener consentimiento informado explícito y declarar los propósitos y plazos de uso. Ambos marcos regulatorios operan sobre la consecuencia — la captura no consentida ya ocurrida — no sobre la causa: la asimetría de información que hace posible que individuos cedan datos biométricos irrevocables sin comprender plenamente las implicaciones.

En América Latina, los marcos equivalentes — LGPD en Brasil, legislaciones similares en Argentina, Colombia, México y Perú — están en proceso de maduración. Ese vacío regulatorio relativo hace especialmente relevante el desarrollo de capacidades individuales de gestión deliberada de la identidad digital, dado que la protección sistémica no opera con la misma efectividad que en jurisdicciones con marcos más consolidados.

5. CONCLUSIONES

El perfil digital de un individuo no es el resultado exclusivo de sus declaraciones conscientes. Es fundamentalmente una construcción inferida por sistemas predictivos a partir de rastros de comportamiento producidos sin autorización deliberada — y esa inferencia tiene consecuencias laborales, financieras, asegurativas y semánticas medibles.

La biometría ocular añade una dimensión cualitativamente nueva a ese problema: la irrevocabilidad. Los datos de comportamiento digital son modificables con esfuerzo y tiempo. Los datos biométricos oculares no lo son. Esa diferencia no es técnica — es ética y operativa, y la literatura académica no la ha abordado con la especificidad que requiere.

La Metacognición 2.0 (Ravello Joo, 2026) y el Modelo de Coherencia Dinámica proporcionan un marco para responder a esa asimetría desde la perspectiva del agente individual. No eliminan la asimetría — la reducen mediante diseño deliberado de las señales que el agente produce para los sistemas que lo clasifican. En el dominio biométrico, esa reducción implica restricción activa de la exposición a sistemas de captura cuyo uso futuro no está garantizado por marcos regulatorios efectivos.

Dijeron que en la mirada está el alma. Ahora es literal — no como alegoría sino como arquitectura de datos. Y a diferencia de casi cualquier otro dato digital, el alma que está en la mirada no se puede cambiar de contraseña.

LIMITACIONES

Este trabajo presenta limitaciones metodológicas que el autor declara explícitamente. La revisión de literatura es narrativa y no sistemática en sentido estricto, lo que introduce sesgo de selección en las fuentes citadas. Los casos de aplicación del MCD en el contexto biométrico son especulativos — el modelo fue desarrollado en el contexto de identidad semántica digital y su extensión al dominio biométrico requiere validación empírica independiente. La regulación sobre biometría evoluciona rápidamente y algunos aspectos del análisis regulatorio pueden quedar desactualizados en el corto plazo. Investigación futura debería abordar la validación empírica del MCD en contextos de gestión de exposición biométrica y el análisis comparativo de marcos regulatorios en América Latina.

REFERENCIAS

- Ajunwa, I. (2022). *Automated video interviewing as the new phrenology*. Scholarship@UNC. University of North Carolina School of Law.
- Anne, N., Blanco, E., Sambah, E., Piper, J., Kiptoo, P., & Lascko, T. (2019). Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in Kenya. *International Journal of Medical Informatics*, 133, 104006. <https://doi.org/10.1016/j.ijmedinf.2019.104006>
- Bhatt, S., Bhatt, U., & Bhatt, S. (2025). A systematic review of iris biometrics in forensic science: Applications and challenges. *Egyptian Journal of Forensic Sciences*, 15, 12. <https://doi.org/10.1186/s41935-025-00431-7>
- Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. *Computer Networks and ISDN Systems*, 30(1-7), 107-117. [https://doi.org/10.1016/S0169-7552\(98\)00110-X](https://doi.org/10.1016/S0169-7552(98)00110-X)
- Calungsod, M. P. D. (2025). Iris scanning: An evaluation of data privacy and security in World App's biometric system. *Cognizance Journal of Multidisciplinary Studies*.
- Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, 20(1), 88-104. <https://doi.org/10.1177/1461444816657096>
- Crihalmeanu, S., & Ross, A. (2012). Multispectral scleral patterns for ocular biometric recognition. *Pattern Recognition Letters*, 33(14), 1860-1869.
- Doke, K. K., Shelke, S., & Raut, S. (2024). A closer look at sclera: Emerging trends in biometric authentication. *IEEE Xplore*.
- Federal Trade Commission. (2014). *Data brokers: A call for transparency and accountability*. Federal Trade Commission. <https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014>
- Grover, A., & Leskovec, J. (2016). node2vec: Scalable feature learning for networks. En *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 855-864). ACM. <https://doi.org/10.1145/2939672.2939754>
- Hu, J., Qin, C., Li, J., Gao, H., & Li, J. (2025). When GDD meets GNN: A knowledge-driven neural approach for entity resolution in property graphs. *Information Systems*.
- Hu, M. (2020). Cambridge Analytica's black box. *Big Data & Society*, 7(2). <https://doi.org/10.1177/2053951720938091>
- Kammerer, B. (2022). The legal implications of artificial intelligence video interviewing. *Iowa Law Review*.
- Kejriwal, M. (2023). Named entity resolution in personal knowledge graphs. *arXiv preprint*. <https://arxiv.org/abs/2307.01557>

- Kulke, L., Feyerabend, D., & Schacht, A. (2020). A comparison of the Affectiva iMotions facial expression analysis software with EMG for identifying facial expressions of emotion. *Frontiers in Psychology*, *11*, 329. <https://doi.org/10.3389/fpsyg.2020.00329>
- Ravello Joo, C. E. (2026). Metacognición 2.0: Diseño deliberado de identidad digital ante sistemas predictivos de inteligencia artificial — El Modelo de Coherencia Dinámica (MCD). *Zenodo*. <https://doi.org/10.5281/zenodo.20092009>
- Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism. *Internet Policy Review*, *11*(3). <https://doi.org/10.14763/2022.3.1670>
- Rodrigues, J. A., Sousa, A., & Carneiro, D. (2026). Advanced consumer behaviour analysis: Integrating eye tracking, machine learning, and facial recognition. *MDPI*.
- Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. *EMBO Reports*, *19*(8), e46579. <https://doi.org/10.15252/embr.201846579>
- Shaw, H., Ellis, D. A., Geyer, K., Davidson, B. I., Ziegler, F. V., & Smith, A. (2022). Subjective reports overstate the relationship between screen time and mental health. *Psychological Science*, *33*(8), 1421-1432. <https://doi.org/10.1177/09567976211040491>
- Wang, Y. Q., Li, X. L., Liao, B., Luo, J., & Cai, L. J. (2021). KG2Vec: A node2vec-based vectorization model for knowledge graph. *PLoS ONE*, *16*(3), e0248552. <https://doi.org/10.1371/journal.pone.0248552>
- Wilcox, A., Damarin, A. K., & McDonald, J. A. (2021). Is cybervetting valuable? *Industrial and Organizational Psychology*, *15*(3), 315-333. <https://doi.org/10.1017/iop.2021.108>

Preprint depositado en Zenodo bajo licencia Creative Commons CC BY 4.0.

Autor: Carlos Eduardo Ravello Joo — ORCID: 0009-0007-5631-7436

Este preprint es el segundo de una serie. El primero está disponible en:

<https://doi.org/10.5281/zenodo.20092009>

Mayo 2026