SISTEMAS BIOMÉTRICOS E INVESTIGACIÓN CRIMINAL.
Fundamentos, modalidades y desafíos.

Autor: Lic. Maffía, Diego M.
Instituto Universitario de la Policía Federal Argentina
Centro de Estudios de Tecnologías Biométricas.

RESUMEN:

Este trabajo analiza el papel de los sistemas biométricos en la investigación criminal, repasando sus fundamentos tecnológicos y las modalidades ya instaladas junto con aquellas en proceso de consolidación. Se destacan las condiciones de uso, las limitaciones de disponibilidad y fiabilidad, y la necesidad de respaldo pericial para garantizar resultados válidos. Asimismo, se subrayan los desafíos técnicos, éticos y procedimentales que enfrenta la disciplina, en un contexto de creciente influencia de la inteligencia artificial y de exigencias de estandarización internacional.

---

1. ¿Qué es la Biometría?

En términos etimológicos, la palabra "Biometría" está conformada por dos partículas de origen griego: Bios (vida) y Metron (medida). Esta certeza, ampliamente utilizada, resulta insuficiente para explicar la complejidad y los alcances actuales de esta tecnología. Aun así, la persistencia de su utilización se explica no solo por la simpleza, engañosa por cierto, sino también en su antigüedad. La aparición en el ámbito académico puede ser rastreada hasta el año 1875, cuando el Dr. Maureau Morris, médico estadounidense, publica el trabajo "*Biometry: its relation to the practice of medicine*" proponiendo la incorporación de métodos cuantitativos y estadísticos en los estudios médicos (Jain y Ross, 2015). El concepto reaparecería a principios del Siglo XX, cuando en 1900 Karl Person y Walter Weldon, a quienes luego se les sumaría nada menos que Francis Galton, fundan la revista "Biometrika". Esa publicación, con el correr de los años, se transformaría en el principal canal impulsor para la incorporación de la Estadística en el mundo científico (Gomez Villegas, 2009).

Durante buena parte del Siglo XX, la palabra estuvo asociada a enfoques y prácticas estadísticas vinculadas al estudio de los seres vivos, no solamente humanos, abarcando entre otras cosas el crecimiento de cultivos, cálculos de masa arbórea, etc. De hecho, aún hoy, la Sociedad Internacional de Biometría (IBS)[1] se presenta en su página web como una organización dedicada "*al desarrollo y la aplicación de la teoría y los métodos estadísticos y matemáticos en las biociencias. Estos campos incluyen la agricultura, la ciencia biomédica, la salud pública, la ecología, las ciencias ambientales, la silvicultura y disciplinas afines*" (IBS, 2026).

Sin embargo, está claro que hoy el uso masivo del término hace referencia a otra realidad. Y posiblemente el inicio de ese cambio se deba a un periodista norteamericano, Andrew Pollack, quien en su columna del New York Times dedicada a tecnología, publicó en el mes de septiembre de 1984 el artículo "*Recognizing the Real You*" en el cual describía el uso incipiente de ciertas tecnologías orientadas al control de acceso. Según Chaudhari et al. (2013), allí aparece utilizada por primera vez la palabra "Biometrics" como asociada a este campo.

[1] https://www.biometricsociety.org/about/who-we-are

Como suele ocurrir con otras palabras en idioma inglés que son traducidas al español, debemos tener en cuenta la diferencia que se establece en aquel idioma, entre "Biometry", "Biometric" y "Biometrics". No en vano Borges nos explicó que el nombre es arquetipo de la cosa. Conforme el Diccionario de Oxford[2], la primera palabra implica "*La medición de los seres vivos y los procesos asociados con la vida, incluyendo la aplicación de las matemáticas, particularmente la estadística, a los problemas de la biología*". Por el adjetivo "Biometric" se entiende aquello "*que utiliza mediciones de características humanas, como los dedos o los ojos, con el fin de identificar a las personas*", mientras que el sustantivo plural "Biometrics" remite a "*una forma de identificar a las personas por sus características físicas únicas, típicamente por razones de seguridad*".

De todos modos, la palabra "Biometría", incluso con estas distinciones que acabamos de hacer, se ha abierto paso a estos nuevos significados. Si tomamos la definición de Anil Jain (2011:2), este la reconoce "*como la ciencia de reconocer a un individuo basándose en las características físicas, conductuales o psicofisiológicas de la persona, ya sea de manera totalmente automatizada o semiautomatizada*". Como vemos, se trata de una definición amplia, que apunta a delimitar un campo específico del conocimiento. Por el contrario, una mirada mucho más instrumental encontramos en la publicación on line del Department of Homeland Security (DHS)[3] de los EEUU, para quien "*la biometría es el reconocimiento automatizado de individuos basado en sus características biológicas y de comportamiento, a partir de las cuales se pueden extraer rasgos biométricos distintivos y repetibles con fines de reconocimiento biométrico. Estas características, a menudo llamadas modalidades, incluyen, entre otras, huellas dactilares, patrones del iris o rasgos faciales que pueden utilizarse para el reconocimiento automatizado*".

Sin perjuicio de estas dos definiciones y de muchas otras similares que podrían citarse, de nuestra parte entendemos que la Biometría, en tanto disciplina aplicada, presenta cuatro características excluyentes: 1) su objeto es la verificación, validación o comprobación de la identidad humana, 2) se mueve dentro de un entorno tecnológico propio, 3) transforma un rasgo humano biometrizable en un valor numérico que permite su rápida comparación con otros similares, y finalmente, 4) trabaja frecuentemente asociado a una base de datos, o al menos en comparación con otro dato biométrico similar.

2. Los "fundamentals" de la Tecnología Biométrica:

En vista del carácter introductorio de este artículo, entendemos que vale la pena repasar algunos conceptos centrales que se vinculan con el funcionamiento de los Sistemas Biométricos. Estas aplicaciones suelen clasificarse según el origen de la característica humana sobre la que han sido construidos. De este modo tendremos, por un lado, los abarcados por la Biometría Fisiológica o Estática (huellas dactilares, rostro, geometría de la mano, características oculares, etc.) y por el otro la Biometría Comportamental (antiguamente llamada "Dinámica") que comprende la dinámica de tecleo, la firma y escritura, la cadencia de paso y otras donde intervenga de una u otra forma algún tipo de conducta o movimiento de la persona. (Kaur et al., 2020)

[2] https://www.oed.com/?tl=true
[3] https://www.dhs.gov/biometrics

También podremos dividir a las aplicaciones en Biometría Dura y Biometría Blanda. La primera hace referencia a sistemas que utilizan toda la información que puede ser extraída de una característica personal, como por ejemplo el Reconocimiento Facial, los AFIS (Automatic Fingerprint Identification System) o la Biometría de la Voz (Prakash et al., 2012). En tanto que la segunda se basa solo en algunas de esas características del rasgo humano completo para extraer información, utilizable pero no determinante para sugerir un resultado de identidad o no identidad. Dentro de esta encontramos la estimación de edad, peso o género basado en rasgos faciales, la detección de idioma en el caso de la voz o la de tipo fundamental en el caso de las huellas dactilares, por ejemplo. Entre otras funciones, la Biometría Blanda aporta soluciones al propio funcionamiento de los sistemas completos por medio de acciones de "clustering", agregando una capa de procesamiento que favorece la tarea posterior de clasificación, búsqueda y comparación (Dantcheva et al., 2015).

Desde el punto de vista de la funcionalidad, los sistemas biométricos están diseñados para dar respuesta a dos preguntas esenciales: a) ¿Esta persona es quien dice ser?, y b) ¿Quién es esta persona? La primera se resuelve comparando dos muestras entre sí y es lo que el vocabulario de la disciplina denomina Verificación, que se suele sintetizar con la expresión 1:1. La actividad ligada al segundo interrogante recibe el nombre de Identificación y se simplifica como 1:N, donde N es el número de componentes de un conjunto de datos determinado (Jain et al., 2011).

Tanto en tareas de Verificación como de Identificación, nos vamos a encontrar con la aparición de otro concepto fundamental: el Umbral. Según Badovinac (2025), se trata de la línea que establecemos para que la aplicación incluya más o menos candidatos (en 1:N) o valide o no una identidad (en 1:1). Esta decisión, generalmente en manos del usuario del sistema, va a depender de múltiples factores como ser el entorno de aplicación, el conocimiento que tengamos de las fortalezas y debilidades del software, la calidad de la muestra suministrada, etc. Íntimamente ligado a esto tenemos otro de los "fundamentals" que venimos recorriendo: la Distancia, que se trata del grado de aproximación entre dos vectores o plantillas biométricas en las que se han convertido los rasgos biometrizables de un ser humano (Jain et al., 2011).

Para entender mejor esto último es conveniente explicar, aunque sea brevemente, como trabaja cualquier sistema biométrico. Su funcionamiento se basa en una serie de pasos a través de los cuales la característica humana involucrada (una huella dactilar, una imagen facial, una muestra de voz, etc.) es "desarmada" en cuanto tal y luego "recreada" bajo un modelo matemático (un vector numérico, una plantilla biométrica). El procesamiento biométrico de un rasgo fisiológico o comportamental de una persona abarca una serie de pasos bien definidos: Detección, Normalización, Extracción de Características, Generación de Plantilla y finalmente Comparación y Decisión. Esta suerte de "traducción" de una particularidad corpórea del mundo real al lenguaje computacional es lo que permite la velocidad de funcionamiento de este tipo de sistemas, aun cuando una muestra se lance a la búsqueda en una base de datos compuesta por millones de especímenes similares.

Los seres humanos poseemos decenas de características fisiológicas o comportamentales, y sin embargo no todas ellas son biometrizables, es decir que puedan resultar útiles para extraer información destinada a validar o sugerir una identidad. Los rasgos humanos utilizados y sus desarrollos tecnológicos asociados, deben cumplir con ciertas condiciones. Entre ellas se destacan la Universalidad (algo que esté presente en todos los individuos), la Unicidad (es decir que tenga características discernibles entre sujetos), la Estabilidad (deben tratarse de

características lo más invariantes posible), la Usabilidad (no solo debe ser de sencilla aplicación sino también facilitar su aceptación por parte del público) y la Fiabilidad (o sea que las tasas de error, aún presentes, sean aceptables).

En este apretado repaso nos resta abordar el tema de los diferentes enfoques científicos que han dominado el campo biométrico desde sus inicios hasta el presente. A partir de la década de 1960 en adelante, y motivados por razones de índole práctica, agencias policiales y de inteligencia de EE.UU. y de la entonces Unión Soviética comenzaron a motorizar investigaciones que les permitiera buscar en sus archivos de manera rápida y eficaz huellas dactilares, fotografías faciales o grabaciones de voz y, de ser necesario, compararlas entre sí (Chaudhari et al., 2013).

Desde aquellos comienzos y hasta mediados de la década pasada, la tecnología se basó en el trabajo de algoritmos clásicos que extraían la información de las muestras suministradas por medio de mediciones, reducción de dimensionalidad y clasificación estadística (de allí el nombre de "Enfoque Estadístico"). Esto sufrió un giro radical con la introducción del paradigma de Entrenamiento basado en el aprendizaje profundo y las redes neuronales, es decir campos pertenecientes a la Inteligencia Artificial. La influencia de la IA no ha sido homogénea en los sistemas biométricos. En tecnologías más maduras, como la dactilar y en cierto grado la de la voz, sus aportes, aunque lograron mejorar las prestaciones frente a muestras complejas, no tuvo tintes revolucionarios. En cambio, en el terreno del Reconocimiento Facial no es aventurado sostener que fue el punto de inflexión que le permitió alcanzar el grado de desarrollo de las dos anteriores primero, y luego protagonizar la expansión que vemos en la actualidad.

3. Modalidades biométricas más usuales en el campo de la Investigación Criminal

Como ya dijimos en párrafos anteriores, los sistemas biométricos nos ayudan a responder dos interrogantes ligados a la identidad de una persona. Esos interrogantes, que en definitiva pueden ser resumidos en uno solo (*de quien se trata*, más allá de toda duda razonable), es un desafío constante en una investigación criminal y trasciende el rol que ocupe la persona de interés. Podrá tratarse de una víctima hallada sin vida, o que aún viva no pueda ser identificada adecuadamente (por carecer de documentación o no poder expresarse con normalidad); podrá ser un sospechoso, cuyas imágenes o su voz quedó fijado por algún dispositivo con esa capacidad; o bien podrá asumir el papel de detenido y por lo tanto resulte necesario identificarlo de manera adecuada. Ahora bien, no todas las tecnologías biométricas que han visto la luz hasta ahora pueden incorporarse al espectro instrumental de una investigación criminal. Las razones para ello pasan por:

a) La disponibilidad del rasgo en un entorno de investigación: La biometría basada en las características del iris es una de las mas robustas de las que se han ideado hasta el momento. De hecho, la distribución de sus líneas y la presencia de microformaciones equiparables a las minucias, ponen a este rasgo al nivel de las huellas dactilares. Sin embargo, ¿cuántas veces disponemos de una muestra del iris de una persona durante una pesquisa?
b) El grado de usabilidad de la aplicación: otro sistema que ha demostrado altísimas tasas de acierto es el basado en la localización de los capilares que irrigan la retina. El problema es que su adquisición implica un procedimiento sumamente invasivo, lo que ha impedido el escalamiento de su uso. Y una vez mas volvemos a la pregunta anterior ¿en que circunstancias tendríamos que apelar a un sistema de esta clase en una investigación?

c) La ausencia de bases de datos que puedan utilizarse con fines de identificación: Poseemos bases de datos de escala poblacional tanto de huellas dactilares como de imágenes faciales. Sin embargo, se carece de conjuntos similares para otras características que sí solemos encontrar ligadas a la dinámica investigativa, como ser la cadencia de paso o la escritura. Frente a esta carencia, un sistema biométrico solo podría ser utilizado en aplicaciones de Verificación 1:1 y por lo tanto su aporte solo sería menor.

A estas tres condiciones principales podemos agregar otras también relevantes como ser el nivel de desarrollo e implantación de una tecnología (siendo aquí donde cobra relevancia el concepto de Fiabilidad antes explicado) y la existencia o no de una disciplina forense que la respalde.

De las dieciséis modalidades biométricas reconocidas por el Biometric Institute[4] en sus publicaciones, cuatro ya se encuentran definitivamente instaladas en el campo de la Investigación Criminal y dos han iniciado el camino para convertirse en valiosas herramientas en el mediano plazo.

En el primer grupo encontramos las huellas dactilares, el rostro humano, la voz y el ADN. Con respecto a este último, por supuesto que se corresponde a una característica única y de cuya robustez nadie puede dudar. También es cierto que admite comparaciones 1:1 y tareas de identificación 1:N cuando se cuenta con una base datos genética, tarea que en nuestro país apenas ha comenzado. Sin embargo, su procesamiento discurre por un camino completamente diferente al del resto de los sistemas biométricos cuyo funcionamiento fue descripto en el punto anterior. La secuenciación de ADN posee un equipamiento específico y sus prácticas se enmarcan en una disciplina (la genética) absolutamente diferente a la biometría. En buena medida esto explica por qué no siempre sea asumida como una técnica biométrica pura.

Las dos biometrías que aspiran a convertirse en herramientas de investigación de uso cotidiano son las basadas en la marcha o cadencia de paso y la firma y escritura. Respecto de la primera, ya ha demostrado utilidad como recurso auxiliar, especialmente frente a imágenes de videovigilancia de baja calidad, tomadas a distancia o donde las personas de interés luzcan oclusiones sobre su rostro. Sin embargo, tanto los sistemas biométricos probados hasta ahora, como la disciplina forense comparativa que la respalda aún carecen de la fortaleza necesaria para su incorporación rutinaria. En un reciente trabajo (Liu et al., 2026), se hace mención a las dificultades que aún se enfrentan: ausencia de bases de datos poblacionales representativas, la dependencia de metodologías puramente observacionales y la falta de validación empírica sólida. En pruebas de laboratorio, las tasas de error de los sistemas biométricos aún están por encima del 10%, valor comparable a los sistemas de reconocimiento facial hacia el 2010, previo a incorporación de la IA. Estas circunstancias limitan tanto su utilización como su valor probatorio.

¿Y qué ocurre con la escritura y la firma? Sin duda son elementos protagonistas de investigaciones vinculadas al fraude documental, delitos económicos o suplantaciones de identidad entre otras. Sin embargo, en el campo biométrico aún se adolece de una necesaria falta de estandarización debido a la diversidad de dispositivos de captura. Tengamos en cuenta que no es solo la imagen lo que se analiza, sino que se extrae información de presión, velocidad, aceleración y/o coordenadas espaciales. Aquella diversidad ocasiona que sea difícil

[4] https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

lograr uniformidades mínimas en la información biométrica y por lo tanto se complejiza su implementación como herramienta vinculada a la identificación. En su trabajo, Aytuglu e Islek (2026) ponen énfasis en limitantes adicionales, tales como dificultades de generalización en sistemas entrenados con muestras insuficientes (fruto de bases de datos poco representativas) y tasas de error también por encima del 10%.

El cuadro que sigue puede resultar útil para resumir en que se basan estas diferentes modalidades biométricas mencionadas, las fuentes más comunes en las que podemos encontrar muestras de esa naturaleza y la frecuencia en la que son utilizadas en una Investigación Criminal.

Tipo de Biometría	En qué consiste	Fuentes	Frecuencia de utilización
Huella dactilar	Basado en patrones de crestas y surcos de la yema de los dedos y mapeo de minucias	Fichas dactiloscópicas Rastros latentes Impresiones monodactilares	Alta
Rostro	Rasgos faciales extraídos de imágenes.	Imágenes de videovigilancia o de cualquier otra naturaleza (RRSS, aportes ciudadanos, tareas de investigación, etc)	Alta
Voz	Características acústicas y patrones del habla.	Archivos de audio Interceptaciones telefónicas Otros registros audiovisuales	Media
ADN	Determinación del perfil genético de un individuo. Puede ser nuclear o mitocondrial	Toma directa de persona de interés. Rastros biológicos colectados en escena de hecho. Soportes de uso cotidiano: ropa, utensilios, peines, cepillos dentales, etc	Media
Marcha	Se basa en el patrón físico al caminar o correr y ángulos que forman cadera, piernas, rodillas, tobillos, etc.	Imágenes dinámicas de cualquier naturaleza.	En proceso de consolidación
Firma y Escritura	Verificación mediante trazado temporal. Analiza forma, velocidad y presión.	Manuscritos, libros rubricados, documentación notarial, contratos, etc.	En proceso de consolidación

Fuente: Elaboración Propia

4. El Rol Pericial y la validación de resultados.

En campos de aplicación de alto riesgo, como lo son las investigaciones criminales donde un error acarrea consecuencias siempre negativas, este tipo de soluciones requieren un uso supervisado por personal entrenado y además contar con el respaldo de una práctica forense reconocida. Esta última será la disciplina criminalística correspondiente, cuyos expertos validarán los resultados propuestos por el sistema automático.

Nunca tenemos que perder de vista que los sistemas biométricos deben ser entendidos como medios tecnológicos que en esencia fueron diseñados para acelerar procesos de búsqueda que

antiguamente se realizaban en forma manual, circunstancia evidente sobre todo para el caso de las huellas dactilares y el rostro humano.

Aunque hay matices, casi nunca es necesario contar con el apoyo de un sistema biométrico para realizar un Cotejo 1:1, sino que basta con la formación pericial del experto para determinar si dos huellas dactilares, dos rostros o dos muestras de escritura corresponden o no a la misma persona. En cambio, resultan ser una herramienta fundamental a la hora de efectuar una búsqueda en bases de datos con miles o millones de identidades. Y bajo esta modalidad 1:N de uso es que surge una circunstancia que no debemos olvidar: los resultados de salida son una simple sugerencia, una predicción, no un resultado cerrado. En la práctica, ese output se traduce en una lista de candidatos (cuya extensión dependerá del umbral que hemos elegido, y de allí la importancia del criterio que utilicemos) ordenados según un valor probabilístico calculado por el sistema.

A nivel mundial, la normativa, los manuales de buenas prácticas y los protocolos que han ido apareciendo en los últimos años no hacen mas que repetir una y otra vez, para diferentes modalidades biométricas, la obligatoriedad de confirmar por medio de un estudio forense a cargo de un experto, aquellos resultados proporcionados por una aplicación.

Pero el factor humano no se agota en la intervención pericial. Continúa con la actividad del investigador que tiene a cargo la pesquisa. Este protagonista, debe tomar con precaución los resultados que le son informados, cotejando y contrastando estos datos con otros que ya posea, ya que en definitiva una investigación criminal no es mas que la aplicación del método científico a un terreno en particular, igual que ocurre con la medicina, la biología o la astronomía. Una identificación positiva suministrada por el laboratorio forense involucrado debe ser tomado como un “descubrimiento” o como el resultado de una experimentación. Ese hallazgo abre nuevas líneas de acción que nos ayudarán a confirmarlo o descartarlo: ¿Quién es X? ¿Dónde vive? ¿Registra antecedentes por hechos similares? ¿El celular de X impactó en una antena de la zona del hecho? ¿El vehículo involucrado puede ser vinculado de alguna forma con X? Como vemos, hay mucho mas para hacer con ese “descubrimiento” de lo que a priori se podría suponer. Y a todo este trabajo posterior de investigación, debemos agregar el rol de las autoridades judiciales, quienes no solo deben velar por el cumplimiento de las reglas del debido proceso, sino que también tienen la función (sobre todo el Juez), de interpretar los resultados periciales y de pesquisa a la luz de la sana crítica.

A modo de síntesis y en apoyo a lo que vinimos diciendo en los párrafos precedentes, se ha elaborado el siguiente cuadro, en el que volvemos a encontrar las modalidades biométricas utilizadas en una Investigación Criminal, acompañadas en esta oportunidad por la disciplina criminalística que posee el marco teórico y metodológico adecuado para validar sus resultados. Hemos agregado también el Protocolo que en nuestro país resulta aplicable cuando es así el caso.

Tipo de Biometría	Disciplina Criminalística involucrada	Protocolo
Huella dactilar	Papiloscopía	No
Rostro	Análisis Forense Facial	Protocolo Unificado para la Búsqueda y Comparación Facial (Resolución MINSEG 1234/2026)
Voz	Acústica Forense	Protocolo Único para la Comparación Forense de Voces. (Resolución MINSEG 526/2024)
ADN	Genética Forense	Protocolo para la Obtención de Muestras Biológicas en el Lugar del Hecho, para Determinaciones Genéticas (Resolución MINSEG 1061/2025)
Marcha	Antropometría	No
Firma y Escritura	Scopometría	No

Fuente: Elaboración Propia

5. Desafíos para los Sistemas Biométricos.

La implementación de los sistemas biométricos enfrenta enormes desafíos. En sentido amplio, y más allá de las particularidades de cada uno, su utilización como llave de acceso a nuestra identidad digital los ha vuelto un blanco apetecible para los ataques con fines de suplantación (spoofing). Desde rústicos ataques de presentación por medio de fotografías faciales o huellas dactilares de silicona, hasta creaciones de IA forman hoy parte de la realidad cotidiana. (Europol, 2025).

Las bases de datos que los sostienen, son en su gran mayoría de escala poblacional y se encuentran bajo responsabilidad gubernamental. Al formar parte de la categoría de sistemas críticos (Banco Mundial, 2025) son pasibles de sufrir ciberataques por parte de hackers solitarios u organizaciones criminales. En ese sentido existe una clara obligatoriedad del Estado en preservar los datos biométricos de la ciudadanía, situación que se hace extensible a cuando estos son utilizados aún con fines legítimos como lo es una investigación penal (Ley 25.326, Art. 9 y 22).

Otro gran desafío lo constituye el rol del experto humano (ya detallado en el punto anterior) y la consolidación de sus prácticas criminalísticas. Mientras asistimos a una auténtica revolución tecnológica, protagonizada por las herramientas derivadas de la IA, en paralelo se está desarrollando el lento proceso de reconversión de las ciencias forenses que propone el abandono de metodologías cualitativas y su reemplazo por métodos de análisis cuantitativos. Esta transformación demanda, entre otras acciones, investigación continua, producción de Procedimientos Operativos Estándar, medición de tasas de error pericial y de incertidumbre y por supuesto esfuerzos adicionales de capacitación y equipamiento.

6. Conclusión

Al día de hoy, los sistemas biométricos constituyen una herramienta esencial para la investigación criminal contemporánea. Como vimos, su principal aporte reside en la capacidad de acelerar procesos de identificación y aumentar la fiabilidad de los resultados, siempre en articulación con la labor del experto humano. Al mismo tiempo, el desarrollo de los sistemas biométricos plantea desafíos transversales que exceden a cada modalidad en particular. La protección de las bases de datos poblacionales frente a ciberataques, la necesidad de protocolos estandarizados y la reconversión de las ciencias forenses hacia metodologías cuantitativas son aspectos inseparables a su implementación. En este sentido, el diálogo entre innovación tecnológica, capacitación continua y resguardo de los derechos fundamentales será decisiva para que la biometría siga consolidando su papel como herramienta confiable y legítima en el campo de la investigación criminal.

Bibliografía

Badovinac, N. (2025, February). Optimization of the decision threshold for application in biometric systems under extreme conditions of facial image verification. In Proc. Int. Conf. ACCHE–Challenges of Contemporary Higher Education (pp. 1-6).

Dantcheva, A., Elia, P., & Ross, A. (2015). What else does your biometric data reveal? A survey on soft biometrics. IEEE Transactions on Information Forensics and Security, 11(3), 441–467.

Europol (2025), Biometric vulnerabilities, Ensuring future law enforcement preparedness, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg.

Gómez Villegas, M. Á. (2009). Karl Pearson, el creador de la estadística matemática [Cap. 21]. En J. Basulto Santos, J. J. García del Hoyo y M. D. Pérez Hidalgo (Eds.), Historia de la probabilidad y la estadística (IV) (pp. 351-356). Universidad de Huelva.

Jain, A.K., Ross, A.A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer, New York

Jain, A. K., & Ross, A. (2015). Bridging the gap: From biometrics to forensics. Philosophical Transactions of the Royal Society B: Biological Sciences, 370(1674), 20140254.

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. Medicine, Science and the Law, 60(2), 131-139.

Morris, M. (1875). Biometry: its relation to the practice of medicine. New York: J.F. Trow & Son.

Pollack, A. (1981, September 24). Technology; Recognizing the real you. The New York Times. nytimes.com

Prakash, N., Singh, Y. P., & Rai, D. (2012). Emerging trends of face recognition: a review. World Applied Programming, 2(4), 242-250.

World Bank; International Bank for Reconstruction and Development. (2025). Enhancing the Cyber Resilience of Identification (ID) Ecosystems: Key Risks and Good-Practice Mitigations