JUSTICIA AUTOMATIZADA Y LA EROSIÓN DE LA CAUSA PROBABLE

Un Análisis Crítico del Caso Angela Lipps y el Régimen Jurídico del Reconocimiento Facial en la Investigación Criminal

Equipo redacción Derecho Artificial

DERECHO ARTIFICIAL

TABLA DE CONTENIDOS

INTRODUCCIÓN

En la intersección entre la eficiencia tecnocrática y las garantías constitucionales, el sistema de justicia penal de los Estados Unidos atraviesa una crisis de legitimidad impulsada por la confianza ciega en la infalibilidad algorítmica. El caso de Angela Lipps, una abuela de 50 años residente de Tennessee, constituye un recordatorio perturbador de las consecuencias humanas cuando el juicio humano se subordina a la señal de la máquina[1]. El 14 de julio de 2025, Lipps fue arrestada a punta de pistola por los U.S. Marshals mientras cuidaba a cuatro niños pequeños, bajo una orden de arresto emitida en Fargo, Dakota del Norte —un estado que ella nunca había visitado—, basándose exclusivamente en una coincidencia de un software de reconocimiento facial[2]. A pesar de encontrarse a 1.200 millas de distancia en el momento de los hechos y poseer registros bancarios que confirmaban su presencia en Tennessee, Lipps permaneció encarcelada durante casi seis meses, perdiendo su hogar, su automóvil y su mascota antes de que los cargos fueran desestimados en la víspera de Navidad de 2025[3].

Este error judicial no es un incidente aislado, sino el síntoma de una patología sistémica: el sesgo de automatización y la erosión deliberada del estándar de causa probable. La tecnología de reconocimiento facial (FRT, por sus siglas en inglés), a menudo presentada como una herramienta forense de precisión matemática, es en realidad un sistema de emparejamiento digital que genera "leads" o pistas investigativas, no evidencias definitivas de identidad[4]. En el caso Lipps, al igual que en otros siete casos documentados de arrestos injustos por FRT en el país, la policía omitió labores básicas de investigación —como verificar coartadas o revisar marcas de tiempo en transacciones— al asumir que la "coincidencia" algorítmica era prueba suficiente para privar de libertad a una ciudadana[5].

La tesis central de este artículo sostiene que el uso actual del reconocimiento facial en la investigación criminal ha degradado el estándar constitucional de la Cuarta Enmienda, permitiendo que sospechas puramente tecnológicas sustituyan a la creencia razonable basada en hechos. Mientras la jurisprudencia reciente, como en los casos Carpenter y Riley, ha comenzado a reconocer que "lo digital es diferente"[6], el régimen jurídico que regula la biometría facial sigue siendo un terreno fragmentado y permisivo. La falta de una regulación de lege ferenda que exija corroboración independiente y que reconozca los sesgos demográficos inherentes a estos sistemas

[1]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 686.
[2]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", págs. 393-394.
[3]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 8.
[4]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1026.
[5]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[6]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 472.

—donde las tasas de error son significativamente mayores para mujeres y personas de color— crea un vacío de rendición de cuentas que este trabajo se propone desgranar[7][8].

A lo largo de las siguientes secciones, se ofrecerá un análisis integral comenzando por la anatomía del fallo en Fargo (Parte I), el análisis técnico de las discrepancias demográficas cuantificadas por el NIST (Parte II), y el desafío que esto representa para la doctrina de la expectativa razonable de privacidad (Parte III). Finalmente, propondremos un marco regulatorio basado en la exigencia de órdenes judiciales específicas para el uso de FRT (FRT Warrants) y el fortalecimiento del derecho de confrontación en la era de la inteligencia artificial.

[7]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 60.
[8]Documento "Artificial Intelligence is Putting Innocent People at Risk of Being Incarcerated", pág. 20.

PARTE I. ANATOMÍA DE UN ERROR JUDICIAL: EL CASO DE ANGELA LIPPS EN FARGO

El caso de Angela Lipps representa la culminación de un fracaso sistémico donde la confianza ciega en la tecnología desplazó los protocolos más elementales de la investigación criminal. No se trató simplemente de un fallo técnico en una base de datos, sino de una cascada de negligencias humanas que transformaron una pista digital en una sentencia de privación de libertad de facto.

1.1. LA GÉNESIS DEL ERROR: DE LAS IMÁGENES DE VIGILANCIA A LA IDENTIFICACIÓN POSITIVA

La investigación se originó en 2025, tras un caso de fraude bancario en Fargo, Dakota del Norte, donde una sospechosa utilizó una identificación falsa del Ejército de los Estados Unidos para retirar decenas de miles de dólares[9]. El Departamento de Policía de Fargo procesó fotogramas de las cámaras de seguridad a través de un software de reconocimiento facial[10]. El algoritmo devolvió como coincidencia el perfil de Angela Lipps, una mujer de 50 años residente de Tennessee, a aproximadamente 1.200 millas de distancia del lugar de los hechos[11].

A pesar de la advertencia técnica generalizada de que estos resultados deben ser considerados únicamente como "leads" o pistas investigativas, el oficial encargado procedió a realizar una comparación visual subjetiva[12]. Tras revisar las fotos de la licencia de conducir y las redes sociales de Lipps, el detective redactó en la declaración de la orden de arresto que la sospechosa "parecía ser la acusada basándose en las características faciales, el tipo de cuerpo y el estilo y color de cabello"[13][14]. Este acto de "confirmación visual" por parte del agente no mitigó el error del algoritmo, sino que lo validó mediante un sesgo de confirmación, convirtiendo una probabilidad estadística en una certeza judicial sin soporte empírico adicional.

1.2. EL COLAPSO DE LA LABOR DETECTIVESCA BÁSICA: OMISIÓN DE VERIFICACIÓN DE COARTADAS

La patología más grave en el caso Lipps fue la renuncia voluntaria de la policía a realizar las tareas básicas de detección. Antes de proceder a la detención, los investigadores omitieron deliberadamente verificar la posibilidad física de que Lipps se encontrara en Dakota del Norte[15]. No se realizaron llamadas telefónicas de verificación, ni se

[9]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", págs. 181, 217.
[10]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[11]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 393.
[12]Documento "Incident 1416: Un supuesto error de reconocimiento facial... - AI Incident Database", pág. 626.
[13]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1021.
[14]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 8.
[15]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.

solicitaron registros bancarios o marcas de tiempo de transacciones en su lugar de residencia habitual[16].

Este fenómeno, identificado en otros casos similares como el de Nijeer Parks en Nueva Jersey o Robert Williams en Detroit, sugiere que el uso de software biométrico genera una complacencia automatizada[17]. Los agentes tienden a ignorar evidencias contradictorias o a dejar de recolectar pruebas clave una vez que la máquina ofrece un nombre[18]. En el caso de Lipps, solo después de seis meses de encarcelamiento, cuando su abogado defensor presentó formalmente registros bancarios que probaban su presencia en Tennessee durante el tiempo del fraude, la policía de Fargo procedió a realizar la entrevista que debió ocurrir antes del arresto[19]. Este retraso inexcusable demuestra que, para los investigadores, la señal digital tuvo mayor peso probatorio que la realidad geográfica de la imputada.

1.3. LA ODISEA PROCESAL: DETENCIÓN INTERESTATAL Y EL IMPACTO DEVASTADOR

El 14 de julio de 2025, la vida de Angela Lipps fue desmantelada violentamente. Fue arrestada a punta de pistola por los U.S. Marshals mientras cuidaba a cuatro niños pequeños en Tennessee[20]. Al ser clasificada como fugitiva, fue recluida en una cárcel de Tennessee durante 108 días sin derecho a fianza, antes de ser finalmente extraditada a Dakota del Norte el 30 de octubre de 2025[21][22].

El impacto de este error judicial trascendió lo procesal para convertirse en una catástrofe personal. Durante su medio año de detención injusta, Lipps perdió su hogar, su automóvil y su mascota debido a la imposibilidad de cumplir con sus obligaciones económicas[23][24]. Los cargos no fueron desestimados hasta la víspera de Navidad de 2025, cuando la evidencia de su coartada resultó incontestable[25]. A pesar de la gravedad del error, el Departamento de Policía de Fargo no emitió una disculpa oficial, subrayando una brecha de rendición de cuentas donde el sistema protege su propia infalibilidad tecnológica a costa de la dignidad de los ciudadanos inocentes[26].

---

[16]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 8.
[17]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 393.
[18]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 428 [ref. 1173 del original].
[19]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[20]Documento "Fargo city leaders prepare for possible lawsuit over mistaken identity | KFGO", pág. 619.
[21]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[22]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 393.
[23]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[24]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 10.
[25]Documento "Fargo city leaders prepare for possible lawsuit over mistaken identity | KFGO", pág. 620.
[26]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.

PARTE II. LA BIOMETRÍA SIN CIENCIA: SESGOS DEMOGRÁFICOS Y FALLOS ESTRUCTURALES

La pretensión de que el reconocimiento facial (FRT) opera como una disciplina forense rigurosa, análoga al análisis de ADN, carece de sustento científico empírico en el contexto de la investigación criminal[27]. A diferencia de las pruebas biológicas, la FRT es una tecnología de emparejamiento probabilístico que depende críticamente de la calidad de los datos de entrada y de la integridad del diseño algorítmico. En esta sección, analizaremos cómo la degradación de la imagen y los sesgos demográficos estructurales documentados por el NIST convierten a esta herramienta en una fuente persistente de errores judiciales.

2.1. "GARBAGE IN, GARBAGE OUT": IMPACTO DE LA BAJA CALIDAD DE LAS IMÁGENES

El principio técnico fundamental que rige estos sistemas es el de "Garbage In, Garbage Out" (GIGO): la precisión de la salida algorítmica es directamente proporcional a la fidelidad de la imagen de entrada[28]. En casos como el de Angela Lipps o Nijeer Parks, las "imágenes sonda" (probe images) suelen provenir de cámaras de seguridad de baja resolución, capturadas en ángulos oblicuos, con iluminación deficiente o desenfoque por movimiento[2930].

La investigación ha demostrado que el uso de imágenes degradadas aumenta exponencialmente la tasa de falsos positivos[31]. Resulta particularmente alarmante la práctica policial de "mejorar" manualmente las fotografías para forzar una coincidencia[32]. En el caso Parks, por ejemplo, un analista admitió haber alterado los píxeles de la foto de una licencia de conducir para "aclararla" antes de procesarla en el software, una manipulación que el sistema jurídico a menudo ignora pero que invalida la fiabilidad del resultado técnico[3334]. Al procesar imágenes de mala calidad, el algoritmo tiende a generar "doppelgängers" o candidatos que comparten rasgos genéricos pero no la identidad real, lo que contamina la fase de confirmación humana con una falsa sensación de certeza matemática[35].

---

[27]Documento "A Forensic Without the Science | Center on Privacy and Technology | Georgetown Law".
[28]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 850.
[29]Documento "A Forensic Without the Science | Center on Privacy and Technology | Georgetown Law".
[30]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 876.
[31]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS...", pág. 1022.
[32]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 64.
[33]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS...", pág. 1022.
[34]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS...", pág. 1022.
[35]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community".

2.2. EL ANÁLISIS NIST: DISCREPANCIAS EN TASAS DE ERROR POR RAZA, GÉNERO Y EDAD

El estudio más exhaustivo sobre la materia, el informe NISTIR 8280, confirma que el rendimiento de los algoritmos no es uniforme a través de los grupos demográficos[3637]. Tras evaluar 189 algoritmos comerciales, el NIST cuantificó disparidades masivas en las tasas de falsos positivos, que pueden ser entre 10 y 100 veces mayores para ciertos grupos en comparación con el grupo de referencia (hombres blancos)[3839].

Las conclusiones del NIST son devastadoras para la pretensión de imparcialidad del sistema:

> Género: Los falsos positivos son sistemáticamente más altos en mujeres que en hombres en casi todos los algoritmos probados[40].
>
> Raza: Se documentaron tasas de error significativamente elevadas en personas de ascendencia africana y asiática[41]. Para algunos algoritmos, los rostros de individuos de África Oriental produjeron tasas de coincidencia errónea 100 veces superiores al promedio basal[42].
>
> Edad: La precisión se degrada drásticamente en los extremos del espectro vital, afectando a niños y ancianos con una frecuencia mucho mayor[43].

Estas discrepancias no son meras anomalías estadísticas, sino fallos de diseño[44]. La mayoría de los sistemas han sido entrenados con bases de datos compuestas predominantemente por hombres blancos, lo que resulta en una incapacidad técnica del software para distinguir variaciones sutiles en otros fenotipos, un fenómeno que traslada el sesgo histórico de la sociedad al código informático[4546].

2.3. LA VULNERABILIDAD DE LA MUJER NEGRA: FACTORES PSICOMÉTRICOS Y TÉCNICOS

El caso de Angela Lipps subraya una vulnerabilidad interseccional crítica: la tasa de error para mujeres negras es, a menudo, la más alta de todo el sistema biométrico[4748].

---

[36]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS...", pág. 1017.
[37]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 1.
[38]Documento "What NIST Data Shows About Facial Recognition and Demographics - SIA", pág. 1030.
[39]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 6.
[40]Documento "What NIST Data Shows About Facial Recognition and Demographics - SIA", pág. 1033.
[41]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 2.
[42]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 32.
[43]Documento "What NIST Data Shows About Facial Recognition and Demographics - SIA", pág. 1033.
[44]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 2.
[45]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 887.
[46]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1171.
[47]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 849.
[48]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 890.

Estudios como Gender Shades han demostrado que mientras la tasa de error para hombres blancos puede ser de apenas un 0.8%, para mujeres de piel oscura esta cifra puede escalar hasta el 34.7% o incluso el 47% en tareas de clasificación[4950].

Esta deficiencia técnica se ve agravada por el sesgo de confirmación humana[51]. Cuando un detective recibe una lista de candidatos de la máquina —a menudo cientos de imágenes que el algoritmo ha "puntuado" como similares—, el agente humano tiende a buscar semejanzas superficiales en lugar de inconsistencias[5253]. En el caso Lipps, el detective basó su confirmación visual en el "tipo de cuerpo y estilo de cabello", características que son volátiles y carecen de valor forense de identificación única[54]. Esta combinación de un algoritmo ciego al color y un investigador humano complaciente crea una "tormenta perfecta" de injusticia que priva a los ciudadanos negros de su presunción de inocencia ante el ojo digital[55].

[49]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 48.
[50]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1169.
[51]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1171.
[52]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[53]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 10.
[54]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS...", pág. 1011.
[55]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 8.

PARTE III. EL DESAFÍO CONSTITUCIONAL: LA CUARTA ENMIENDA EN LA ERA DE LA VIGILANCIA DIGITAL

La detención de Angela Lipps no solo expone un fallo en la praxis policial, sino que pone de manifiesto la obsolescencia de los marcos doctrinales tradicionales frente a la potencia de la biometría automatizada. La Cuarta Enmienda, concebida para proteger la seguridad de las personas contra registros y incautaciones irrazonables, se encuentra hoy en una encrucijada interpretativa donde la tecnología ha superado la capacidad de los tribunales para definir qué constituye una "búsqueda" (search) en el siglo XXI[56].

3.1. EVOLUCIÓN DE LA DOCTRINA: DE LA OBSERVACIÓN FÍSICA A LA INTRUSIÓN PERSISTENTE

Históricamente, la doctrina de la Cuarta Enmienda se ha estructurado sobre la premisa de la "expectativa razonable de privacidad" establecida en Katz v. United States (1967)[57]. Bajo este prisma, lo que un individuo expone voluntariamente al público no goza de protección constitucional, asumiendo que "el rostro no es un misterio para el mundo"[58]. Sin embargo, la Corte Suprema ha comenzado a reconocer que en la era digital la acumulación masiva de datos públicos altera la naturaleza misma de la privacidad.

En el caso Riley v. California (2014), el tribunal dictaminó unánimemente que "lo digital es diferente", subrayando que los dispositivos modernos no son meros objetos físicos, sino depósitos de la totalidad de la vida de una persona[59]. Esta distinción cualitativa y cuantitativa es fundamental para el análisis del reconocimiento facial: mientras que un oficial puede observar un rostro en una multitud, la FRT permite procesar miles de rostros simultáneamente, comparándolos contra bases de datos globales en milisegundos[60]. Posteriormente, en Carpenter v. United States (2018), la Corte amplió esta visión al exigir una orden judicial para acceder a datos de localización celular (CSLI), argumentando que el rastreo persistente y retrospectivo de los movimientos de un ciudadano crea un registro "omnipresente" que los redactores de la Constitución no habrían tolerado[61]. La FRT, aplicada a redes de cámaras de vigilancia, opera de manera análoga al CSLI, permitiendo una vigilancia que es profunda, amplia y automática[62].

---

[56]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", págs. 430, 462.
[57]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 195.
[58]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 466.
[59]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 863.
[60]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 435.
[61]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 956.
[62]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 473.

3.2. PRINCIPIOS DE "FUTURE-PROOFING": ANTI-AGREGACIÓN Y ANTI-RASTREO

Para abordar la brecha entre la norma y la tecnología, la academia jurídica ha propuesto principios de "blindaje futuro" (future-proofing) derivados de la jurisprudencia reciente[63]. Estos principios sugieren que el análisis constitucional no debe centrarse en la tecnología específica, sino en el impacto sistémico de la vigilancia:

> Principio de Anti-Agregación: Sostiene que, aunque la captura de una sola imagen facial pueda ser inocua, la recopilación sistemática y el emparejamiento de miles de estas imágenes para crear un historial de vida constituye una intrusión que viola la Cuarta Enmienda[64].
>
> Principio de Anti-Permanencia: Cuestiona la capacidad del Estado para almacenar indefinidamente datos biométricos y realizar búsquedas retrospectivas. El uso de la FRT como una "máquina del tiempo" que permite a la policía reconstruir los movimientos pasados de Angela Lipps —o de cualquier ciudadano— sin sospecha individualizada, rompe con el carácter transaccional de la investigación criminal clásica[65][66].
>
> Límite a la Vigilancia Permeante: La Corte en Carpenter y Jones advirtió contra una vigilancia policial "demasiado permeante" que enfría las libertades de asociación y expresión[67][68]. Cuando el rostro se convierte en una baliza digital rastreable, el espacio público deja de ser un lugar de anonimato práctico para convertirse en una red de monitoreo absoluto que "corre contra todos", no solo contra los sospechosos[69].

3.3. TENSIÓN ENTRE EXPECTATIVA RAZONABLE DE PRIVACIDAD Y EXPOSICIÓN PÚBLICA

El desafío dogmático central reside en la "paradoja del rostro". Tradicionalmente, los tribunales han sostenido que la observación de algo expuesto a la vista del público no constituye un registro[70]. No obstante, existe una diferencia fundamental entre ser visto por un transeúnte y ser identificado, catalogado y rastreado por un algoritmo[71].

El anonimato en público es una condición necesaria para la libertad en una sociedad democrática. La FRT desmantela esta "oscuridad práctica" al vincular instantáneamente el cuerpo físico con la identidad digital y el historial administrativo

---

[63]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", págs. 421-422, 477.
[64]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", págs. 483-484.
[65]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", págs. 485, 487.
[66]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 198.
[67]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 491.
[68]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 196.
[69]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 495.
[70]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 195.
[71]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 522.

de una persona[72]. En el caso de Angela Lipps, la policía de Fargo operó bajo la presunción de que el uso del software no requería una orden judicial previa porque las imágenes provenían de una cámara de seguridad en un lugar público[73]. Sin embargo, al aplicar los principios de Carpenter, se argumenta que el uso de biometría para identificar a Lipps a 1.200 millas de distancia constituye un registro constitucionalmente significativo, ya que revela información que de otro modo sería "incognoscible" para la labor policial ordinaria[74][75]. La Cuarta Enmienda debe, por tanto, interpretarse como una barrera contra la automatización de la sospecha, exigiendo que el "match" algorítmico sea tratado no como el fin del proceso probatorio, sino como una herramienta que requiere el mismo nivel de supervisión judicial que un registro físico de un hogar[76].

[72]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 585.
[73]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 8.
[74]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 487.
[75]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 390.
[76]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 217.

PARTE IV. LA CRISIS DE LA CAUSA PROBABLE: FRT COMO "INVESTIGATIVE LEAD" VS. EVIDENCIA

La detención de Angela Lipps y otros ciudadanos injustamente señalados por algoritmos plantea una interrogante doctrinal de primer orden: ¿en qué medida una coincidencia biométrica automatizada puede satisfacer el estándar constitucional de "causa probable"? La práctica policial actual sugiere una peligrosa tendencia a tratar el "match" de una máquina no como una pista inicial, sino como una prueba de culpabilidad casi concluyente, subvirtiendo la lógica de la Cuarta Enmienda[77].

4.1. EL ESTÁNDAR FLORIDA V. HARRIS: ¿ES FRT ANÁLOGO AL OLFATO CANINO?

En la jurisprudencia estadounidense, la validez de las herramientas tecnológicas para establecer causa probable suele compararse con el uso de perros detectores de narcóticos, regulado por el caso Florida v. Harris (2013)[78]. Bajo este estándar, el tribunal debe evaluar si, bajo la "totalidad de las circunstancias", la señal de la herramienta es suficientemente fiable para que una persona de prudencia razonable crea que existe evidencia de un crimen[79].

Sin embargo, la analogía entre el olfato canino y el reconocimiento facial (FRT) resulta insuficiente y engañosa[80]. Mientras que un perro detector opera bajo un entrenamiento binario (presencia o ausencia de olor), la FRT es un sistema digital que gestiona identidades humanas con sesgos demográficos incrustados, donde los fallos de entrada (inputs) —como imágenes borrosas o bases de datos no diversas— producen fallos de salida (outputs) desproporcionados según la raza o el género[81][82]. La doctrina jurídica ha señalado que las herramientas de vigilancia digital merecen un nivel de escrutinio judicial superior al de las herramientas analógicas, precisamente por su capacidad para generar sospechas masivas basadas en datos defectuosos[83][84].

[77]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 850.
[78]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 870 [ref. 141 del original].
[79]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 871.
[80]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 876.
[81]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", págs. 850, 876-877.
[82]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 2.
[83]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 878.
[84]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 473.

4.2. EL PELIGRO DEL SESGO DE AUTOMATIZACIÓN: SUBORDINACIÓN DEL JUICIO HUMANO

El caso Lipps ilustra con crudeza el fenómeno de la complacencia automatizada[85]. Este sesgo cognitivo lleva a los agentes de la ley a confiar excesivamente en los resultados de los sistemas automáticos, incluso cuando estos contradicen la lógica más elemental[86]. En Fargo, el detective encargado no solo aceptó la sugerencia del software, sino que la "validó" mediante una comparación visual subjetiva que el TAISE Knowledge Hub califica explícitamente como un sesgo de confirmación[87].

El agente redactó en la orden de arresto que Lipps "parecía ser la sospechosa", ignorando que el software solo había proporcionado un "lead" o candidato de una lista probabilística[8889]. Esta tendencia de los oficiales a confiar en el algoritmo por encima de la labor de investigación básica —como verificar coartadas o buscar pruebas físicas independientes— es lo que permitió que Lipps fuera arrestada a 1.200 millas del lugar del crimen[9091]. La "señal" de la máquina, por muy débil que sea su puntuación de similitud (similarity score), tiende a eclipsar la evidencia exculpatoria en la mente del investigador[92].

4.3. PROPUESTA DOGMÁTICA: INSUFICIENCIA DEL "MATCH" ALGORÍTMICO PARA CAUSA PROBABLE

Desde una perspectiva de lege ferenda, la tesis que defendemos es que un resultado de reconocimiento facial es, por definición, insuficiente para sustentar causa probable por sí solo[93]. Los propios formularios de solicitud de FRT utilizados por diversas agencias suelen incluir advertencias explícitas: "Pista investigativa, no causa probable para realizar un arresto"[9495].

Varios estados ya han comenzado a codificar esta distinción. Por ejemplo, la legislación de Alabama, Virginia y Massachusetts prohíben explícitamente el uso de resultados de

[85]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1026 [ref. 12 del original].
[86]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 13.
[87]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[88]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 8.
[89]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 10.
[90]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", págs. 8-9.
[91]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[92]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", págs. 1021, 1026.
[93]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 850.
[94]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 11.
[95]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1021.

FRT como la única base para una orden judicial o un arresto[9697]. Para que el sistema recupere su integridad epistémica, es imperativo que la coincidencia algorítmica sea tratada exclusivamente como un punto de partida que exige corroboración independiente[98]. En el caso de Lipps, si se hubiera aplicado este principio, una simple revisión de sus registros bancarios en Tennessee habría detenido el proceso antes de que se emitiera la orden de arresto injusta[99]. La Cuarta Enmienda exige una creencia razonable basada en hechos, y una probabilidad estadística generada por un software opaco no puede sustituir la obligación constitucional del Estado de conectar de manera independiente a una persona con un crimen[100].

[96]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 210 [nota 140 del original].
[97]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 210 [nota 139 del original].
[98]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 390.
[99]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 389.
[100]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 850.

PARTE V. PATRONES SISTÉMICOS DE INJUSTICIA: ANÁLISIS COMPARADO DE CASOS

El encarcelamiento de Angela Lipps no es una anomalía estadística, sino el octavo caso documentado en los Estados Unidos donde la tecnología de reconocimiento facial (FRT) ha servido como catalizador para la privación injusta de la libertad[101]. Esta serie de fracasos revela una patología estructural en la que el error algorítmico no es corregido, sino amplificado por la praxis policial. En esta sección, analizaremos la jurisprudencia del error a través de casos emblemáticos y extraeremos los denominadores comunes que definen esta crisis de integridad judicial.

5.1. LA SERIE DE FRACASOS: DE DETROIT A NUEVA JERSEY Y GEORGIA

La geografía del error biométrico en Estados Unidos traza un mapa de negligencia procesal. El caso de Robert Williams en Detroit marcó un hito; fue arrestado frente a su familia por un robo que no cometió, basándose en una coincidencia errónea que el sistema judicial no cuestionó hasta después de su detención[102]. Detroit, tras acordar una indemnización de 300.000 dólares, ahora exige evidencia independiente antes de cualquier arresto basado en FRT, una lección aprendida a un alto costo humano[103].

En la misma jurisdicción, el caso de Michael Oliver ilustra el peligro de utilizar software con tasas de error alarmantes. Oliver fue detenido por un sistema que, según estimaciones del propio jefe de policía, fallaba en la identificación en un 96% de los casos[104]. Por su parte, Nijeer Parks, en Nueva Jersey, pasó diez días encarcelado tras una "identificación" algorítmica de baja calidad, a pesar de encontrarse a millas de distancia del lugar de los hechos[105][106].

Más recientemente, el caso de Quran (Randal) Reid en Georgia subraya la dimensión interestatal del problema: Reid fue arrestado en Atlanta por un robo en Luisiana, un estado que nunca había visitado[107]. Al igual que Lipps, Reid insistió en que nunca había pisado la jurisdicción del crimen, pero la policía omitió verificar su presencia física en su lugar de trabajo en Georgia antes de proceder al arresto[108]. Un patrón similar se observa en el caso de Porcha Woodruff, arrestada con ocho meses de embarazo por un robo ocurrido semanas antes, a pesar de que el video de vigilancia mostraba a una sospechosa que claramente no estaba embarazada[109].

---

[101]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[102]Documento "Artificial Intelligence is Putting Innocent People at Risk of Being Incarcerated", pág. 20.
[103]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[104]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 183 [ref. 12 del original].
[105]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1026 [ref. 51 del original].
[106]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 11.
[107]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[108]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[109]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 13.

5.2. EL DENOMINADOR COMÚN: NEGLIGENCIA Y INVISIBILIZACIÓN TECNOLÓGICA

Al analizar estos casos en conjunto, surgen dos factores críticos que explican por qué la FRT se traduce en detenciones ilegales:

A. El colapso de la fase de confirmación humana: En todos los casos citados, la policía arrestó a ciudadanos sin conectarlos de manera independiente con el crimen[110]. Existe un fenómeno de complacencia automatizada donde el investigador, al recibir una lista de candidatos de la máquina, busca similitudes visuales para validar el "lead" en lugar de buscar inconsistencias que lo descarten[111][112]. En el caso de Michael Oliver, una investigación básica habría revelado que él poseía numerosos tatuajes visibles que el sospechoso en el video no tenía[113]. En el caso de Parks, el analista alteró manualmente los píxeles de la foto para "aclararla", forzando una coincidencia que la realidad técnica no sustentaba[114].

B. La invisibilización ante el magistrado: Existe una tendencia alarmante a ocultar el uso de la FRT en las declaraciones juradas para órdenes de arresto[115]. En el caso Parks, el detective omitió mencionar que la sospecha nació de un algoritmo; en su lugar, utilizó términos inventados como "comparación de alto perfil" para sugerir una certeza científica inexistente[116][117]. El detective ignoró deliberadamente las advertencias impresas en los formularios de solicitud de FRT que especifican: "PISTA INVESTIGATIVA, NO CAUSA PROBABLE PARA UN ARRESTO"[118].

Esta invisibilización tecnológica impide que el magistrado ejerza su función de control constitucional. Si el juez no sabe que la identificación proviene de un software probabilístico con sesgos demográficos —y que además se basó en imágenes de baja resolución—, no puede evaluar la razonabilidad de la causa probable[119]. El sistema, por tanto, permite que una señal digital opaca se "lave" a través de una declaración policial subjetiva, transformando un error técnico en un acto de estado indiscutible hasta que la evidencia exculpatoria es demasiado abrumadora para ser ignorada[120].

---

[110]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.
[111]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1170 [ref. 366 del original].
[112]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1021 [ref. 12 del original].
[113]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 13.
[114]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1022.
[115]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 959.
[116]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1011.
[117]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1015.
[118]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 11.
[119]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1016.
[120]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 217.

PARTE VI. HACIA UN MARCO DE CONTROL: REGULACIÓN DE LEGE FERENDA

La insuficiencia de la Cuarta Enmienda para contener la expansión del reconocimiento facial (FRT), evidenciada en la Parte III, exige una respuesta legislativa que establezca un "techo" de protección sobre el "suelo" constitucional[121]. La tragedia de Angela Lipps demuestra que, en ausencia de reglas claras, la policía optará por el camino de la menor resistencia técnica, sacrificando la integridad del proceso penal en aras de una eficiencia mal entendida.

6.1. LA ORDEN DE RECONOCIMIENTO FACIAL (FRT WARRANT)

La primera propuesta dogmática es la creación de una Orden Judicial de Reconocimiento Facial (FRT Warrant)[122]. Dada la capacidad de esta tecnología para rastrear movimientos y asociaciones de forma retroactiva y omnipresente, su uso no debe quedar al arbitrio policial[123]. Se propone un estándar de causa probable reforzada o "causa probable-plus", similar al exigido por la Ley de Intervenciones Telefónicas (Wiretap Act)[124].

Este marco regulatorio debería incluir tres pilares fundamentales:

Limitación por Gravedad: El uso de FRT para identificación debe restringirse exclusivamente a delitos graves o felonías violentas, evitando que una herramienta de vigilancia masiva se utilice para faltas menores que pondrían en riesgo a gran parte de la población[125][126].

Declaración de Necesidad: La solicitud de la orden debe incluir una declaración jurada que certifique que no existen otros medios de investigación menos intrusivos disponibles o que estos han fracasado[127].

Protocolos de Minimización: La orden debe especificar las medidas tomadas para minimizar la captura e identificación de ciudadanos inocentes que aparezcan en el material visual procesado, evitando que una búsqueda individualizada se convierta en una red de arrastre generalizada[128][129].

Jurisdicciones como Alabama, Colorado y Virginia ya han sentado precedentes al prohibir legislativamente que un "match" algorítmico sea la única base para una orden de arresto, exigiendo evidencia corroborativa independiente[130][131].

---

[121]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1197.
[122]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 181.
[123]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1154.
[124]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1202.
[125]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 213.
[126]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1200.
[127]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1202.
[128]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1202.
[129]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 217.
[130]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 210 [nota 140 del original].
[131]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 9.

6.2. TRANSPARENCIA ALGORÍTMICA Y DERECHO DE CONFRONTACIÓN

El sistema de justicia debe garantizar que el uso de IA no se convierta en una "caja negra" inexpugnable para la defensa[132]. Basándonos en la doctrina de Transparencia Forense, defendemos que toda la información generada por el software de FRT es potencialmente exculpatoria y debe estar sujeta a revelación obligatoria bajo Brady v. Maryland[133][134].

En el caso de Angela Lipps, si la fiscalía hubiera estado obligada a entregar la lista completa de candidatos generada por el software —que a menudo incluye cientos de imágenes—, la defensa podría haber demostrado la fragilidad de la identificación inicial[135][136]. La transparencia debe alcanzar:

> La Lista de Candidatos: El acusado tiene derecho a conocer quiénes fueron los otros "posibles matches" descartados subjetivamente por el agente[137].
>
> Puntuaciones de Similitud: Es imperativo revelar el similarity score. Un "match" con una puntuación baja, como ocurrió en el caso de Nijeer Parks, es un indicador crítico de falta de fiabilidad que el magistrado debe conocer[138][139].
>
> Manipulación de Datos: Cualquier alteración de la imagen original (aclarado de píxeles, interpolación, uso de doppelgängers) debe constar en acta, ya que estas prácticas invalidan la base científica del resultado[140][141].

6.3. RESPONSABILIDAD INSTITUCIONAL Y CIERRE DE LA BRECHA DE RENDICIÓN DE CUENTAS

Finalmente, es necesario cerrar la brecha de rendición de cuentas que permite que departamentos de policía eludan su responsabilidad tras un error catastrófico[142]. El caso de Fargo es paradigmático: se privó de libertad a una ciudadana durante seis meses sin una disculpa oficial ni compensación automática[143].

Proponemos un marco de responsabilidad basado en el Examen Humano Significativo (Meaningful Human Review)[144]. Estados como Utah y Colorado ya exigen que cualquier

---

[132]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1016 [nota 29 del original].
[133]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 16.
[134]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1209.
[135]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 10.
[136]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1021.
[137]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 16.
[138]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1011.
[139]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 10.
[140]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1022.
[141]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 390.
[142]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 10.
[143]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[144]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 213.

coincidencia algorítmica sea verificada de forma independiente por al menos dos examinadores entrenados, y que cualquier discrepancia detenga el proceso de identificación[145][146]. Además, el incumplimiento de estos protocolos de entrenamiento y supervisión debe generar responsabilidad institucional bajo la doctrina Monell, reconociendo que la falta de políticas sobre tecnologías de vigilancia constituye una negligencia deliberada que viola los derechos constitucionales[147][148]. Solo mediante la imposición de costos legales significativos y la obligación de verificar coartadas antes del arresto, el sistema podrá transitar de una justicia automatizada hacia una justicia humana y garantista[149].

CONCLUSIÓN

La odisea de Angela Lipps no debe interpretarse como un fallo anómalo en la maquinaria del Estado, sino como el resultado lógico de una arquitectura judicial que ha permitido que la conveniencia tecnológica eclipse la garantía constitucional[150]. El hecho de que una ciudadana pueda ser privada de su libertad durante casi seis meses, perdiendo su hogar, su automóvil y su mascota, basándose en una coincidencia algorítmica a 1.200 millas de distancia de su residencia, revela una fractura profunda en la aplicación del estándar de causa probable[151][152].

A lo largo de este análisis, hemos demostrado que el reconocimiento facial (FRT), lejos de ser la ciencia forense infalible que la retórica policial sugiere, es un sistema probabilístico cargado de sesgos demográficos estructurales. Los datos del NIST confirman que las tasas de falsos positivos son drásticamente superiores en mujeres y personas de color, convirtiendo el uso no regulado de esta tecnología en un motor de desigualdad procesal[153][154]. Como se ha argumentado, el sistema jurídico actual padece de una complacencia automatizada que permite a los agentes de la ley "lavar" la sospecha algorítmica a través de una revisión humana puramente subjetiva, ocultando a menudo el origen tecnológico de la identificación ante los magistrados[155][156].

---

[145]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 214.
[146]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 213.
[147]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 983 [ref. 30 del original].
[148]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1027.
[149]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", pág. 10.
[150]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1107.
[151]Documento "Facial Recognition False Positives: The Lipps Case - DEV Community", pág. 388.
[152]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.
[153]Documento "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects - NIST", pág. 2.
[154]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 850.
[155]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", págs. 1021, 1026.
[156]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 13.

La Cuarta Enmienda, interpretada bajo la luz de casos como Carpenter y Riley, debe evolucionar para reconocer que el rostro no es simplemente una imagen pública, sino la baliza digital de nuestra identidad biométrica[157]. La vigilancia persistente y el rastreo retrospectivo permitidos por la FRT requieren un marco de protección que trascienda el anonimato práctico del pasado[158]. Por ello, este artículo defiende que el "match" algorítmico nunca puede constituir causa probable por sí solo; debe ser tratado exclusivamente como un investigative lead o pista que impone al Estado la obligación ineludible de realizar una corroboración independiente antes de cualquier arresto[159][160].

El caso Lipps, al ser el octavo error de este tipo documentado en el país, subraya el vacío de rendición de cuentas reinante[161]. Sin una regulación de lege ferenda que exija la emisión de órdenes judicales específicas (FRT Warrants), garantice la transparencia algorítmica bajo la doctrina Brady y establezca consecuencias legales para la negligencia institucional, el sistema de justicia seguirá operando bajo una presunción de culpabilidad digital[162][163].

En última instancia, la legitimidad del proceso penal en la era de la inteligencia artificial depende de nuestra capacidad para mantener al ser humano como el eje central de la decisión judicial. La eficiencia nunca debe ser el precio de la dignidad humana. La tragedia personal de Angela Lipps, quien caminó libre en la víspera de Navidad de 2025 solo después de que su vida fuera desmantelada, es una advertencia de que la justicia automatizada es, en esencia, una justicia deshumanizada[164]. El derecho debe actuar ahora para asegurar que la señal de la máquina nunca vuelva a sustituir el juicio razonado de un hombre o una mujer de ley.

[157]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1131.
[158]Documento "Facial Recognition and the Fourth Amendment - Minnesota Law Review", pág. 1199.
[159]Documento "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest", pág. 850.
[160]Documento "Facial Recognition Technology U.S. Commission on Civil Rights... - ACLU", pág. 11.
[161]Documento "AI Facial Recognition Wrongful Arrest – 6 Months in Jail | byteiota", págs. 9-10.
[162]Documento "The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants", pág. 181.
[163]Documento "UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY NIJEER PARKS... - ACLU-nj.org", pág. 1016.
[164]Documento "TAISE Knowledge Hub | AI Safety & Security Education", pág. 684.

BIBLIOGRAFÍA SELECCIONADA Y FUENTES DOCUMENTALES

I. DOCUMENTOS TÉCNICOS Y ESTÁNDARES GUBERNAMENTALES

National Institute of Standards and Technology (NIST). NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Grother, P., Ngan, M., & Hanaoka, K. (Diciembre, 2019).

National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) Part 2: Identification. Grother, P., et al. (2023).

II. JURISPRUDENCIA Y LITIGACIÓN

American Civil Liberties Union (ACLU) & ACLU of New Jersey. Amicus Curiae Brief in Support of Plaintiff's Opposition to Defendants' Motion for Summary Judgment. Nijeer Parks v. John E. McCormac, et al. Caso No. 2:21-cv-04021.

Center on Privacy and Technology | Georgetown Law. A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations. Garvie, C. (2022).

III. DOCTRINA ACADÉMICA

Ferguson, Andrew Guthrie. Facial Recognition and the Fourth Amendment. Minnesota Law Review, Vol. 105 (2021).

Benedict, T.J. The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest. Washington and Lee Law Review, Vol. 79 (2022).

Jones, Allison. The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants. The University of Memphis Law Review, Vol. 56 (2025).

IV. REPOSITORIOS DE INCIDENTES Y REPORTES

AI Incident Database. Incident 1416: Un supuesto error de reconocimiento facial... Angela Lipps.

TAISE Knowledge Hub. US Grandmother Wrongly Imprisoned 6 Months Due to Facial Recognition Misidentification.

Byteiota. AI Facial Recognition Wrongful Arrest – 6 Months in Jail.