Cartapacio
Reseñas bibliográficas y jurisprudencia comentada

Revista Pensamiento Penal
Sección medios digitales y delitos informáticos
Vol. 1, núm. 1 – 2025, págs. 99–118
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/z8fbe249

El derecho a confrontar la prueba de cargo ante las nuevas tecnologías de datos

Comentario al fallo «State v. Corey Pickett» del Tribunal Superior de Nueva Jersey

Tomás Pomar[1]

Resumen

El comentario se refiera al caso *State v. Pickett*, dictado por la Corte Suprema de Nueva Jersey, que marca un punto de inflexión en la jurisprudencia estadounidense sobre la admisibilidad de nuevas tecnologías en el proceso penal. El objeto del caso fue la aceptación de la evidencia de cargo generada por *TrueAllele*, un software de genotipificación probabilística. La defensa objetó la falta de acceso al código fuente del programa para su control. El debate abarcó cuestiones estructurales relacionadas con la transparencia, la auditabilidad y el control judicial de herramientas tecnológicas con pretensión probatoria. El precedente alerta sobre los riesgos de delegar funciones esenciales del Estado en tecnologías opacas desarrolladas con fines comerciales, y subraya la necesidad de establecer estándares públicos rigurosos para su admisibilidad. Inaugura así un debate ineludible: cómo compatibilizar los avances de la ciencia de datos con los pilares constitucionales del proceso penal, asegurando que la innovación no comprometa las garantías tradicionales que sostienen un juicio justo e imparcial.

Sumario

Fallo comentado

Suprema Corte de Nueva Jersey, División Apelaciones, «State of New Jersey v. Corey Pickett», 3/2/2021. Exp. No. A-4207-19T4

Palabras clave

derecho de defensa – genotipificación probabilística – confrontación de la prueba – garantías procesales – secreto comercial – tecnologías en el proceso penal

[1] Abogado especialista en Derecho Informático por la Universidad de Buenos Aires (UBA). Docente de las asignaturas Derecho constitucional y Justicia digital en la Facultad de Derecho de la UBA. Presidente del Observatorio de Derecho Informático Argentino (ODIA) y autor de diversas publicaciones. Correo electrónico: tfpomar@gmail.com

1. Introducción

En el último decenio, el sistema de justicia ha experimentado profundas transformaciones como consecuencia del empleo de nuevas tecnologías. Más allá de la digitalización de las actuaciones judiciales y la consiguiente reconfiguración de los tribunales en espacios virtuales, se ha promovido el desarrollo de herramientas tecnológicas y normativas destinadas a dotar de mayor eficacia a los procesos judiciales como respuesta a la creciente intermediación digital de nuestras vidas. Sin embargo, esta transición de forma y fondo no ha estado exenta de desafíos. Las modificaciones en la práctica tribunalicia han generado nuevas controversias. Muchas de estas, lamentablemente, han dado lugar a pujas bifocales en la que el debate se ve reducido a la supuesta contradicción entre la idea de «innovación» y las tradicionales prácticas institucionales del derecho. Asimismo, vale resaltar que el desconocimiento en materia de informática y/o sistemas por parte de los diversos operadores jurídicos ha dificultado dotar de sustancialidad a estos intercambios, los que terminan por circunscribirse a un nivel de usuario. Es así que, ante nuestra mirada, se configura un escenario casi inédito para el razonamiento jurídico. Por un lado, surgen planteos que se inspiran en un supuesto espíritu «innovador» como forma de pensar el derecho; por el otro, se defiende cierta ortodoxia de prácticas institucionales que, en realidad, no alcanzan siquiera un siglo de madurez. Todo esto ocurre ante los diversos operadores jurídicos que, aún cuando inmersos en las dinámicas de esta época, enarbolan su conocimiento jurídico como justificación para evitar analizar el mundo que los rodea. En este orden de ideas, vale resaltar que esta mecánica ante la «innovación tecnológica» ha caracterizado también, las medidas de investigación empleadas por los Ministerios Públicos Fiscales los que, en sistemas de tipo acusatorio, tienen a su cargo establecer las medidas de prueba a realizarse en el marco de una investigación.

En este contexto, el presente comentario al fallo se propone como objetivo sumar a estos debates específicamente a partir del estudio de las condiciones exigibles para la admisión de nuevas tecnologías con idoneidad probatoria en el proceso penal. A tal fin, dada la intersección entre tecnología y derecho procesal en que el *thema decidendum* se halla, se propone un enfoque de carácter interdisciplinario a fines de abordar adecuadamente el caso.

El fallo objeto de análisis representa un ejemplo paradigmático de los desafíos que plantea la interacción entre tecnología y derecho procesal penal. En particular, se aborda la utilización de *TrueAllele*, un software de genotipificación probabilística, como medio de prueba en un proceso penal. El caso pone de manifiesto cuestiones esenciales relativas a los estándares de admisibilidad de la prueba científica, el rol de los peritos expertos, la transparencia de los métodos empleados y el equilibrio entre la eficiencia tecnológica y la protección de los derechos fundamentales pero, también, respecto al rol de los jueces.

El análisis no solo permite reflexionar sobre los criterios necesarios para evaluar la validez y confiabilidad de las tecnologías aplicadas en el ámbito penal, sino también sobre como las garantías procesales resultan un óbice determinante de los modelos tecnológicos a implementar. El debate aquí planteado adquiere toda su gravitación ante el presente escenario en el que los diversos avances tecnológicos, sin perjuicio de su pretendida eficientización, se presentan, también, como elementos con la capacidad de comprometer principios constitutivos del proceso judicial tales como el derecho de defensa y la igualdad de armas entre las partes.

Así, el presente trabajo ahondará tanto en aspectos técnicos que hacen al funcionamiento del software, como en los diversos elementos jurídicos involucrados en el caso a fines de contribuir al debate por una interpretación que permita compatibilizar la innovación tecnológica con los valores esenciales que hacen al proceso judicial.

2. Hechos del caso

Nueva Jersey, Estados Unidos, 16 de abril de 2017; dos hombres, presuntamente identificados como Corey Pickett y Jonathan Ferrara, se aproximan a un grupo de personas y abren fuego en simultáneo, sin una razón aparente. Una persona pierde la vida al recibir un disparo en la cabeza, mientras que una niña de 10 años resulta herida de bala en el abdomen. Tras el ataque, los sospechosos fueron arrestados por las fuerzas policiales a pocas cuadras del lugar de los hechos. Durante el rastreo de las vías de escape, la policía encontró una pistola Colt .45 en la ruta seguida por Ferrara; y un revólver Smith & Wesson .38 junto a un pasamontañas en la ruta elegida por Pickett.

En el marco de la investigación, los equipos forenses detectaron la presencia de amilasa (un componente de la saliva) en el pasamontañas. Además, se recogieron muestras de ADN de ambas armas y del cargador de la Colt .45. Estas evidencias fueron enviadas al laboratorio policial para su análisis; sin embargo, los estudios preliminares determinaron que las muestras eran insuficientes para realizar un análisis genotípico tradicional. Por otro lado, el pasamontañas contenía dos muestras de ADN, ambas compuestas por perfiles genéticos mixtos. Tras comparar estos perfiles con muestras obtenidas de los sospechosos, se determinó que Corey Pickett era el «contribuyente principal» en ambas mezclas. No obstante, este resultado no constituía prueba suficiente para afirmar que Pickett había utilizado la máscara en el momento del crimen.

Ante esta falta de certeza y considerando que las muestras genéticas halladas en las armas eran demasiado pequeñas para un análisis tradicional, los forenses enviaron el material genético a una empresa privada, *Cybergenetics Corp. Laboratory* (en adelante, *Cybergenetics*). Esta empresa desarrolló y patentó un software innovador llamado *TrueAllele*, diseñado para analizar mezclas genéticas complejas o muestras de tamaño reducido. El programa utiliza un modelo matemático para calcular la probabilidad estadística de coincidencia entre perfiles genéticos. En este caso, *TrueAllele* «logró» identificar coincidencias relevantes entre los materiales genéticos, lo que permitió presentar cargos contra Pickett. Este hallazgo, sin embargo, dio lugar a un debate sobre la admisibilidad y fiabilidad de la evidencia obtenida mediante este software, planteando cuestiones clave sobre las reglas aplicables para la incorporación de nuevas tecnologías en los procesos judiciales.

3. Los software de genotipificación probabilística

En los procesos penales, el ADN tiene un rol protagonista como medio de prueba por su capacidad de establecer coincidencias entre el material genético recolectado en la escena de un crimen y los perfiles genéticos de las personas imputadas. Cabellos, sangre o saliva suelen ser los elementos clave recolectados en el lugar de los hechos, que posteriormente se envían a laboratorios para su análisis. Tradicionalmente, este trabajo se realizaba por parte de especialistas en la materia mediante el método clásico de

genotipificación, una técnica que ha sido el estándar desde su introducción en los tribunales en los años 80.[2]

El método tradicional de genotipificación consiste en identificar diferencias en la composición genética de una persona mediante la comparación en laboratorio de secuencias de ADN. Sin embargo, no siempre se dispone de muestras ideales: cuando el material genético resulta escaso o está mezclado con ADN de varias personas, la metodología convencional pierde eficacia. Es ante este tipo de situaciones donde la tecnología informática ha provisto con una herramienta que supuso un salto significativo.

En las últimas décadas, la genotipificación probabilística ha irrumpido como una solución innovadora para los casos en que no resultaba posible utilizar el método tradicional. En lugar de valerse únicamente del resultado de laboratorio, este procedimiento utiliza algoritmos matemáticos avanzados para calcular la probabilidad de que una muestra de ADN pertenezca a una persona en particular, esto incluso cuando las condiciones del material recolectado resultan adversas: mezclas complejas, cantidades mínimas de ADN, o, incluso, ambas. Estos sistemas prometen mayor precisión, objetividad y rapidez, revolucionando la forma en que se analiza el material genético en el ámbito judicial.

No obstante, el análisis de este tipo de muestras más pequeñas plantea nuevos desafíos, especialmente en lo referente a la custodia y trazabilidad de la prueba. Entre los riesgos más destacados se encuentra la posible «inclusión» de moléculas (la detección de fragmentos de ADN contaminantes que no formaban parte de la muestra original) o la «exclusión» (la omisión de ADN legítimo debido a la insuficiencia de material para el análisis). Dada la naturaleza probabilística de esta técnica, estos riesgos adquieren una relevancia considerable, ya que los resultados, al basarse en estimaciones estadísticas, pueden estar sujetos a interpretaciones diversas.

En términos prácticos, mientras que el análisis tradicional se basa en la observación humana directa de marcadores genéticos, los softwares como *TrueAllele* procesan estos datos a través de modelos algorítmicos que convierten el material biológico en probabilidades estadísticas. Por ejemplo, el programa puede calcular cuán probable es que el ADN de un individuo esté presente en una mezcla en comparación con el ADN de un individuo aleatorio. En definitiva, una estadística genética que arroja probabilidades y cuya auditoría resulta extremadamente dificultosa.

a. TrueAllele

El software *TrueAllele*, desarrollado por el laboratorio privado *Cybergenetics*, es uno de los software de referencia global que utilizan la técnica de genotipificación probabilística. Con más de una década de uso y participación en más de 500 casos penales en diferentes estados de EE.UU., *TrueAllele* ha demostrado su utilidad en situaciones donde el método tradicional no resulta aplicable. A su vez, otros modelos como *STRmix*, utilizado desde 2012 en miles de casos en EE.UU., Europa, Reino Unido y Australia, dan cuenta de la creciente incorporación de este tipo de herramientas en los procesos penales a lo largo y ancho del mundo.

El caso propuesto para su estudio pone en el centro del debate el uso de *TrueAllele*, sus características e implicaciones jurídicas: ¿Puede un modelo algorítmico probabilístico

[2] Crown Court (UK), «Colin Pitchfork», 1988.

ser incorporado como prueba en el marco del proceso penal? ¿Qué garantías asisten al acusado para cuestionar la metodología empleada? Y, sobre todo, ¿Hasta qué punto los avances tecnológicos pueden integrarse de manera equilibrada con los principios fundamentales del derecho? Estas preguntas no son menores.

Aunque *TrueAllele* y otros softwares similares ofrecen promesas de eficacia, vale preguntarse por las condiciones y garantías específicas de desarrollo a las que una herramienta informática debiera ajustarse para que su incorporación al Poder Judicial sea compatible con los principios, garantías y reglas sobre los que se erige el adecuado proceso.

b. Naturaleza jurídica del software

TrueAllele fue el resultado de décadas de evolución tecnológica aplicada al ámbito forense. Fundada en 1994 por el Dr. Mark Perlin, *Cybergenetics* fue una empresa que desde sus inicios se propuso desarrollar herramientas avanzadas orientadas a ser implementadas para realizar estudios genéticos. En pocos años, *TrueAllele* se consolidó como un modelo destacado en la genotipificación probabilística. Su primer uso en los tribunales tuvo lugar en 2009[3], y desde entonces se ha utilizado ampliamente como herramienta probatoria en procesos penales.

El debate sobre *TrueAllele* y el caso *Pickett* no puede abordarse sin antes analizar el contexto histórico que hace a la naturaleza jurídica del software. En los años sesenta, la separación entre hardware y software trajo consigo la necesidad de definir el marco regulatorio aplicable a estos nuevos sistemas informáticos[4]. Si bien inicialmente se exploró la posibilidad de proteger el software mediante patentes, esta opción fue descartada debido a las características particulares de los programas informáticos. Eventualmente, el sistema de derechos de autor se impuso como el modelo preferido por su simplicidad, bajo costo y carácter automático. Tal decisión supuso que cada desarrollador pudiera establecer distintos tipos de licencias para sus obras según su propio criterio. Esto sentó en gran medida las bases de un modelo legal que posibilita la coexistencia de dos modelos distintos para el desarrollo y registración de los sistemas: el software de código cerrado/privativo y el software de código abierto o libre. El primero, como en el caso de *TrueAllele*, se caracteriza por restringir el acceso, uso y modificación del código fuente del sistema, mientras que el segundo busca garantizar la libertad y transparencia mediante licencias más abiertas.

El código fuente es el conjunto de líneas de texto que expresan, en un lenguaje de programación determinado, los pasos que debe seguir el computador para la ejecución de un software específico. Para ser ejecutado por el ordenador, debe ser traducido a lenguaje binario de modo que el hardware puede ejecutar esas órdenes. El resultado de esta traducción, la cual se realiza a través de compiladores o intérpretes o programas similares, se denomina código objeto. Tal como sostiene Beatriz Buseniche «Los programas en código fuente, escritos por programadores y comprensibles para otras personas que dominan la técnica, contienen una intención comunicativa subyacente y pueden existir, incluso, independientemente de la existencia de una máquina. El texto fuente de los programas tiene una capacidad expresiva, es el vehículo idóneo para

[3] Pennsylvania Superior Court, «Kevin James Foley», 2012.
[4] Pomar, 2022.

comunicar algoritmos, soluciones a problemas, de la misma manera que un músico comunica a sus pares la composición mediante la escritura de partituras»[5]

Es decir, el código fuente es la obra cuyo autor es el programador, protegida por los derechos de autor. Podemos advertir que esta es una diferencia fundamental con cualquier otra obra registrable dentro de este sistema: no es posible pensar en situaciones análogas respecto del texto de un libro, una pintura, una fotografía, etc. dado que en estos casos la obra protegida está exhibida; mientras que en el software privativo el funcionamiento del sistema no es revelado. Al respecto, vale tener presente una particularidad diferenciadora del software con otras tantas obras autorales como, por ejemplo, una obra musical. Y es que, si bien el autor de una canción no se encuentra obligado a proporcionar la partitura de la pieza musical a todo aquél que adquiera la reproducción de su obra, esta puede puede ser «interpretada» y «deducida» por cualquier músico con la capacidad suficiente para escribir la partitura luego de escuchar la obra. Esto no sucede con el código fuente de un sistema privativo en que el código fuente (instrucciones que hacen al funcionamiento interno del sistema) no pueden ser deducidas.

El acceso al código fuente permite, entre otras cosas, comprender cómo el software fue diseñado y cuáles son las reglas introducidas por el desarrollador para su funcionamiento. Ahora bien, si no tenemos acceso al código, solo podemos usar el programa, no podemos ver cómo está hecho o introducir mejoras. Un paralelismo muy utilizado es el de la receta de cocina, en que el código fuente sería las instrucciones que permiten confeccionar un plato. Sin la receta solo se puede degustar el plato, pero no sabemos si, al añadir algo, vamos en contra de alguno de sus ingredientes, ya que se desconoce su composición y la proporción[6].

La no publicidad del código fuente es una característica propia de las licencias de tipo privativo de fuerte predominancia en los software de uso diario. Su modelo se basa en limitar los derechos del usuario al mínimo posible, por lo que todas las actualizaciones y modificaciones estarán a cargo del desarrollador quien suele cobrar por ellas. No es menor el hecho de que esta gran limitación de los derechos de los usuarios implica un alto grado de opacidad respecto del funcionamiento del software, en tanto, al desconocerse el modo en que fue programado, no puede tenerse certeza respecto del tipo de seguridad que utiliza ni del tipo de operaciones que realiza. Es por ello que el proveedor del software propietario, como medio para asegurarse de que el usuario cumplirá con la prohibición de no modificarlo, se limita a entregar una copia del código objeto del software (es decir, la que permite ejecutarlo), pero no proporciona al usuario la versión una copia del código fuente, y que trata de preservar en secreto.

Si bien existe una rama dentro de la ingeniería en informática que se dedica a estudiar y desarrollar procesos de traducción inversa (de código objeto a código fuente), se sostiene que no es posible realizar una traducción completamente satisfactoria. Por tanto, el proveedor de software entrega una versión que solamente puede ser ejecutada por el ordenador, es decir, ofrece una versión «encriptada» mientras que su creación, que se encuentra protegida por los extensos derechos de autor, permanece oculta. Incluso, en las licencias de uso de tipo privativas, en las cuales se suele estipular que el usuario se compromete a utilizar el software dentro del marco de los términos y condiciones que se indican en el contrato, es frecuente encontrar cláusulas que prohíben expresamente la

[5] Busaniche, s.f.
[6] Culebro Juárez *et. al.*, 2006.

utilización de la ingeniería inversa[7], a fin de traducir el código objeto a un código fuente entendible por humanos. Así, vemos como la introducción de los programas informáticos dentro del régimen de los derechos de autor plantea retos e impone un conjunto de particularidades al sistema. Esta característica del software resulta un punto esencial para entender la controversia planteada en la decisión judicial bajo estudio.

	Software Libre	Open Source	Software Privativo
Ver el código fuente	✔ 01010101	✔ 01010101	✘ Prohibido
Estudiar el código fuente	✔ 01010101	✔ 01010101	✘ Prohibido
Modificar el código fuente	✔ 01000001	✘ No garantizado	✘ Prohibido
Compartir con otras personas	✔ Compartirlo con otras personas	✔ Solo a veces	✘ Prohibido
Compartir tus modificaciones con otros	✔ Modificaciones con otras personas	✘ No garantizado	✘ Prohibido
Uso comercial	✔ Hacer uso comercial	✘ Prohibido	✘ Prohibido
Uso propietario	✔ Utilizarlo con cualquier propósito	✔ Uso limitado	✔ Solo con permiso del fabricante

Gráfico: Tomás Pomar

4. El desafío de las licencias de software en el proceso penal

En el caso «*State vs. Pickett*», la defensa solicitó acceso al código fuente del software *TrueAllele* con el propósito de contraexaminar al testigo experto, desarrollador del modelo, cuya declaración sustentaba la fiabilidad del programa. Sin embargo, este pedido fue denegado en primera instancia, amparándose en las restricciones impuestas por las licencias privativas utilizadas por *Cybergenetics* para proveer el software al Estado. Este hecho plantea un problema crítico: ni el juez, ni la fiscalía, ni la defensa pueden auditar o comprender plenamente cómo el software alcanza sus conclusiones, ya que el código fuente permanece inaccesible.

Desde su primera aceptación en un tribunal en 2009, *TrueAllele* se ha utilizado bajo la afirmación de su creador, el Dr. Mark Perlin, de que «los estudios de validación son las mejores pruebas de la fiabilidad de los códigos fuente». En 2014, Perlin defendió la objetividad del software, sosteniendo que «cuando resuelve genotipos, nunca considera una referencia o un sospechoso». Sin embargo, ese mismo año, otro modelo de genotipificación probabilística, *STRmix*, fue objeto de críticas judiciales tras detectarse errores de codificación que generaban resultados engañosos, obligando a la empresa

[7] A modo de ejemplo, vale señalar la cláusula 17 de los términos y condiciones de Adobe la cual establece que, "Ciertos elementos de los Servicios y el Software constituyen nuestra información confidencial (o la de nuestros licenciantes). Excepto en los casos expresamente permitidos en los Términos, no debes (ni permitir que terceros): (A) modificar, portar, adaptar o traducir ninguna parte de los Servicios o del Software; (B) realizar ingeniería inversa (incluyendo, pero no limitado a, la supervisión o el seguimiento de las entradas y salidas que fluyen a través de un sistema o una aplicación para recrear dicho sistema), descompilar, desensamblar o intentar de cualquier otra forma descubrir, dentro de cualquier Servicio o Software, el código fuente".

desarrolladora a revelar su código fuente. Asimismo, un informe de *ProPublica*[8] en 2017 señaló problemas similares en el software *Forensic Statistical Tool* (FST), utilizado por laboratorios forenses en Nueva York, cuestionando la fiabilidad de sus resultados probabilísticos.

Más allá de estos antecedentes, es fundamental destacar que estos softwares están diseñados específicamente para su uso en procesos penales, contextos donde los derechos fundamentales, como la defensa en juicio, exigen un nivel adicional de transparencia. En este sentido, el uso de programas con licencias privativas —que impiden el acceso al código fuente incluso bajo acuerdos de confidencialidad— genera tensiones significativas en un ámbito eminentemente público. Como señala Glauco Giostra, la publicidad procesal no es un elemento externo o accesorio al sistema judicial, sino un principio que transforma la validez política y ética de la administración de justicia[9]. Bajo esta lógica, la primacía del derecho de propiedad intelectual sobre las garantías constitucionales, como el derecho de defensa y, específicamente poder confrontar la prueba de cargo, amenaza con socavar los pilares del debido proceso.

5. La audiencia de *discovery* en el derecho procesal estadounidense

A fines de abordar el caso bajo estudio resulta necesario formular algunas aclaraciones previas con respecto a las reglas que dan forma al proceso de tipo acusatorio en los Estados Unidos de América. Esto, a efectos de circunscribir adecuadamente la etapa preparatoria del juicio en la que tuvo lugar el debate sobre los derechos y garantías del acusado en relación con las licencias de software en el proceso penal. En este antecedente, adquieren relevancia constitucional las reglas aplicables a la figura del denominado «*testigo experto*» y los estándares para la admisibilidad de pruebas científicas.

En los Estados Unidos, el sistema procesal penal se basa en un modelo *acusatorio* que busca garantizar la *transparencia* y la *igualdad de armas entre las partes*, principios que adquieren particular relevancia en el desarrollo de pruebas científicas o técnicas. Dentro de este modelo, las etapas del proceso están diseñadas para proteger los derechos del acusado y prevenir desequilibrios en el acceso a la información o las evidencias. El proceso tiene comienzo cuando el fiscal reúne evidencias suficientes para presentar cargos formales ante un Tribunal de Distrito. Este acto incluye una descripción detallada de los hechos, las pruebas disponibles y los cargos imputados. Posteriormente, el acusado comparece en una audiencia inicial, donde se le informa sobre los cargos en su contra, se le asigna un abogado si no cuenta con uno, y se determina si permanecerá detenido o será liberado hasta el juicio.

En este contexto, la etapa intermedia conocida como Discovery adquiere especial importancia. Durante esta fase, ambas partes —fiscalía y defensa— intercambian información relevante para la preparación del juicio. Este procedimiento busca evitar el llamado «*Trial by ambush*» (juicio por emboscada) al garantizar que ambas partes puedan desarrollar estrategias legales adecuadas con pleno conocimiento de las pruebas y testigos que se presentarán en el juicio. Además, el fiscal tiene la obligación de proporcionar a la defensa todas las pruebas en su poder, incluidas aquellas que podrían ser exculpatorias.

[8] Kirchner, 2017, 4 de septiembre.
[9] Giostra, 1989, p. 55

Este principio, conocido como la «*Divulgación Brady*» (*Brady v. Maryland*, 1963), establece que retener evidencia favorable al acusado violaría los principios fundamentales de justicia, ya que el fiscal debe actuar no solo como acusador, sino también como garante de un proceso justo. En palabras del cimero tribunal de Estados Unidos, el fiscal no debe ser **«***el arquitecto de un procedimiento que no se ajusta a las normas de justicia***»**[10]**.**

En los juicios penales, los testigos desempeñan roles esenciales en el desarrollo de los hechos y en la validación de las pruebas. Según su naturaleza, pueden clasificarse en testigos *legos*, quienes ofrecen relatos de hechos presenciados; *testigos de concepto*, quienes aportan información por su relación cercana con las partes o las víctimas; y *testigos expertos*, quienes poseen formación técnica o científica que les permite interpretar y validar pruebas complejas. En el caso bajo estudio, la figura del *testigo experto* adquiere una dimensión especial, ya que el Dr. Mark Perlin, creador del software *TrueAllele*, no solo actúa como experto técnico sino también como desarrollador y comercializador del modelo en cuestión. Esta doble función plantea dudas legítimas sobre su imparcialidad, especialmente en contextos donde la transparencia y la objetividad se suponen como pilares fundamentales del proceso.

En el marco del caso *State v. Pickett*, el fiscal informó durante el Discovery su intención de presentar evidencia científica basada en *TrueAllele*. Sin embargo, debido a que el software aún no había sido validado como prueba admisible en Nueva Jersey, el juez ordenó una audiencia preliminar para determinar su fiabilidad y así poder decidir si se la admitía para declarar en juicio junto con dicha prueba . En dicha audiencia, el Dr. Perlin fue citado como testigo experto para defender la validez del método de genotipificación probabilística empleado. La defensa, por su parte, cuestionó la admisibilidad de la prueba solicitando acceso al código fuente de *TrueAllele* y a otros datos técnicos que permitieran realizar un contrainterrogatorio efectivo. Argumentaron que sin esta información no podrían evaluar adecuadamente la fiabilidad del software ni refutar las afirmaciones del testigo experto. La solicitud fue denegada en primera instancia, lo que llevó al caso a una segunda instancia judicial.

La controversia en el caso *Pickett* refleja una tensión entre dos principios fundamentales: el derecho del acusado a un juicio justo, donde pueda confrontar acabadamente la prueba de cargo para poder defenderse, y la protección de la propiedad intelectual del software. Mientras que *Cybergenetics* argumentó que el acceso al código fuente comprometería sus secretos comerciales, la defensa sostuvo que sin dicha información era imposible evaluar la fiabilidad de la prueba científica. En última instancia, la cuestión radica en si los secretos comerciales pueden prevalecer sobre los derechos constitucionales del acusado, especialmente en casos donde la prueba técnica podría ser determinante para el veredicto. La decisión de denegar el acceso al código fuente de *TrueAllele* plantea interrogantes críticos sobre el equilibrio entre la innovación tecnológica y las garantías constitucionales, un tema que será explorado con mayor detalle en los próximos apartados.

[10] USSC, «Brady v. Maryland», 1963.

6. Estándares aplicables a la incorporación de prueba científica en el derecho procesal de los EE.UU

a. Los estándares «*Frye*» y «*Daubert*» para determinar admisibilidad de la prueba científica novedosa

Dentro del marco del Discovery, etapa preparatoria del juicio, se pueden establecer audiencias específicas para decidir sobre la admisibilidad de pruebas de carácter técnico o científico. En estas audiencias, un testigo experto es citado para acreditar la fiabilidad de la prueba en cuestión. Como hemos señalado previamente, el juez puede aplicar distintos estándares de evaluación para determinar la aceptabilidad de la evidencia técnica presentada. Estos estándares, que varían según las jurisdicciones estaduales, presentan diferencias sustanciales en cuanto a su enfoque y requisitos. Para encuadrar el contexto procesal en el que se sitúa el caso bajo estudio, resulta pertinente explicar los dos principales estándares aplicables: *Frye* y *Daubert*, sin perjuicio de que en este caso particular se haya aplicado el primero debido a que el estado de Nueva Jersey sigue esta doctrina.

El estándar *Frye*, introducido por el caso *Frye v. United States*[11] (293 F. 1013, D.C. Cir. 1923), fue el primero en ser implementado por el sistema judicial estadounidense para regular la admisibilidad del testimonio de expertos sobre *evidencias técnicas o científicas novedosas*. Según *Frye*, la evidencia debe ser «generalmente aceptada como confiable por la comunidad científica a la que pertenece». Este enfoque, aunque sencillo y directo, confía en la validación de la comunidad científica como criterio principal de admisibilidad. Estados como California, Illinois, Maryland, Minnesota, Nueva Jersey, Nueva York, Pensilvania y Washington continúan aplicando este estándar en sus tribunales.

Sin embargo, a partir de recomendaciones relacionadas con la aceptación y credibilidad científica, y específicamente tras el caso *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (509 U.S. 579, 1993), se comenzó a implementar el denominado estándar «Daubert» en los tribunales federales y en más de la mitad de los estados. Aunque no se trata de un cambio sustancialmente opuesto a *Frye*, *Daubert* establece un conjunto de pautas más detalladas para admitir el testimonio de expertos científicos, superando la mera «aceptación general» de *Frye*. Este enfoque se articula en torno a los siguientes principios:

El juez como guardián: Según el Reglamento Federal de Evidencia, la Regla 702 asigna al juez que preside el juicio la responsabilidad de garantizar que las pruebas cumplan con las directrices científicas necesarias.

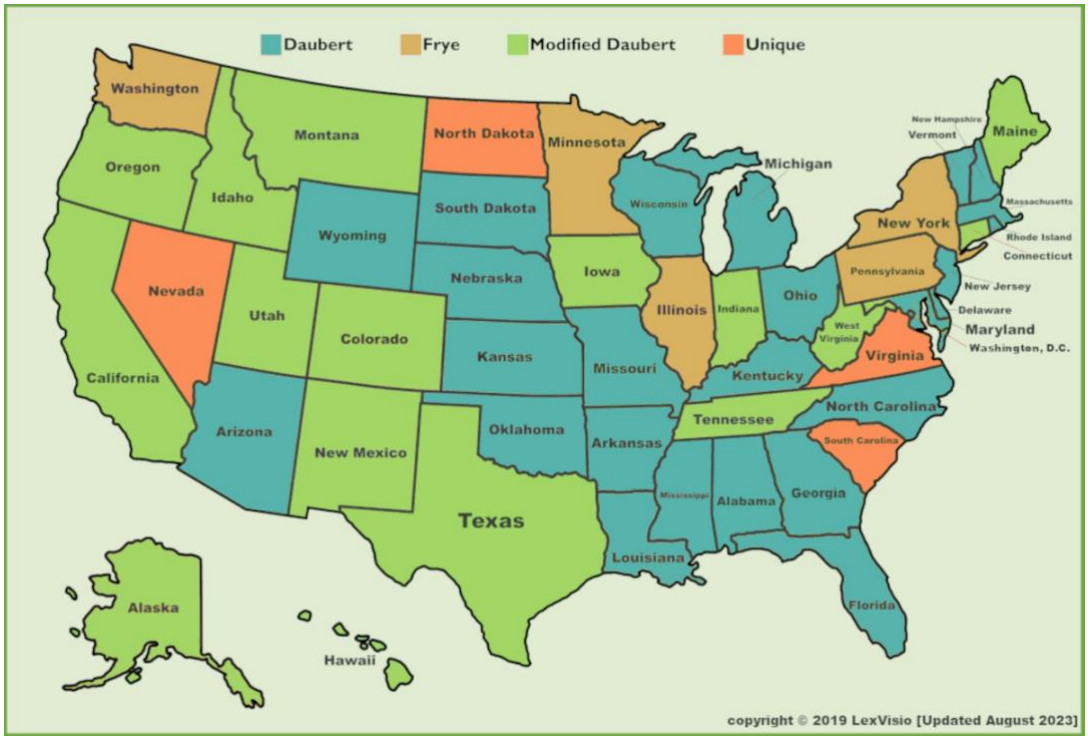
Relevancia y confiabilidad: El juez debe asegurarse de que el testimonio del perito sea «relevante para la tarea en cuestión» y que esté fundamentado en una base confiable.

Conocimiento científico como método científico: Las pruebas admitidas deben cumplir con estándares científicos actuales, demostrando que sus hallazgos se obtuvieron mediante protocolos específicos que se consideran métodos científicos estandarizados.

Factores ilustrativos: Daubert establece criterios adicionales para evaluar el método científico, entre los cuales destacan:

[11] Capellino, 2024, 10 de julio.

- Si la técnica o teoría en cuestión es generalmente aceptada (como indica *Frye*).
- Si los resultados han sido objeto de revisión por pares en publicaciones científicas.
- Si los resultados pueden ser replicados y comprobados mediante análisis o pruebas adicionales.
- Si las pruebas o investigaciones se realizaron de manera independiente al litigio en cuestión.



Fuente: https://www.lexvisio.com/article/2019/07/09/the-states-of-daubert-after-florida

La distinción más evidente entre *Frye* y *Daubert* radica en el alcance de este último. Mientras que *Frye* se enfoca esencialmente en la aceptación general dentro de la comunidad científica, *Daubert* amplía el análisis al incorporar múltiples factores que permiten al juez asumir un rol activo como «guardián» de la admisibilidad de las pruebas. Este enfoque empodera al juez para evaluar no solo la confiabilidad de las técnicas empleadas, sino también su relevancia en el caso particular. Así, mientras *Daubert* anima a los jueces a determinar la admisibilidad, *Frye* se centra en la propia comunidad científica de la cual el perito experto forma parte.

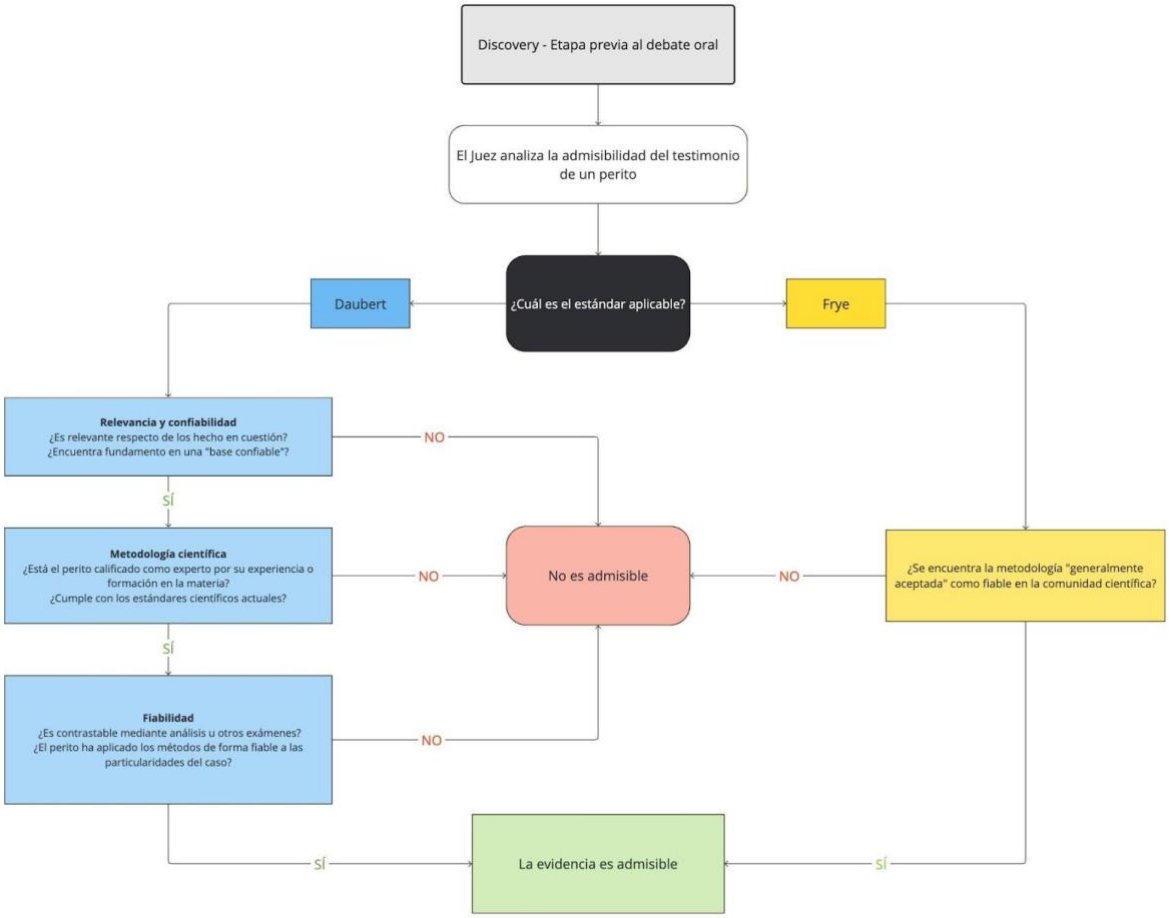


Gráfico: Tomás Pomar

Resulta interesante reflexionar que, hipotéticamente, la aplicación del estándar Daubert en este caso podría haber ofrecido un marco más robusto para evaluar la admisibilidad de la prueba científica. Daubert, al asignar al juez un rol activo como «guardián» de la evidencia, permite un análisis más amplio y crítico de los métodos empleados y su confiabilidad, en lugar de depender exclusivamente de la aceptación general por parte de la comunidad científica. En contraste, bajo Frye, aunque el juez mantiene la decisión final sobre la admisión de la prueba, esta se ve significativamente influenciada por la opinión de la comunidad científica relevante.

En este caso particular, el peso otorgado a la comunidad informática plantea un desafío adicional, ya que la misma está representada en gran medida por actores vinculados directamente con el desarrollo del software *TrueAllele*. El Dr. Perlin, creador del software y testigo experto propuesto por la Fiscalía, encarna esta dualidad al ser el desarrollador de la herramienta licenciada bajo software propietario y, al mismo tiempo, el responsable de defender su fiabilidad. Este conflicto de intereses podría haber sido abordado de manera más adecuada de haberse aplicado el estándar Daubert y, así, exigir un análisis que trascienda la mera aceptación general y contemple cuestiones como la imparcialidad, los métodos empleados y la replicabilidad de los resultados.

7. Planteos de las partes

a. Argumentos de la defensa

Es importante recordar que los jueces del estado de Nueva Jersey, donde se desarrolla el proceso, aplican el antes descrito estándar Frye para evaluar el testimonio de peritos; el testigo experto en genética forense fue el Dr. Perlin, cofundador de la empresa Cybergenetics, desarrolladora de *TrueAllele*. Dicho software fue utilizado para analizar muestras de material genético insuficientes para ser procesadas mediante métodos tradicionales. El modelo de genotipificación probabilística implementado estimó que el ADN del acusado coincidía con las muestras recolectadas, constituyendo así la base de la acusación.

Ante la falta de precedentes que avalaran la confiabilidad de *TrueAllele* en la jurisprudencia local, el Juez fijó una audiencia bajo el estándar *Frye* a fines de determinar su admisibilidad en el proceso. En esta audiencia, el testigo experto debía demostrar que el método de análisis empleado era generalmente aceptado por la comunidad científica de genética forense, a la cual pertenece.

La defensa, en ejercicio del derecho del imputado a controvertir las pruebas presentadas en su contra, solicitó acceso al código fuente del software *TrueAllele*. Según argumentó, el pleno acceso a esta información era un requisito esencial en un sistema contradictorio, ya que resultaba indispensable para realizar un contraexamen efectivo del testimonio del testigo experto. La defensa también enfatizó que sin dicho acceso no podía evaluar ni cuestionar adecuadamente las afirmaciones de la fiscalía.

En concreto, la solicitud incluía «todas las dependencias de software, como bibliotecas de código de terceros, cajas de herramientas y *plug-ins*», así como «materiales de ingeniería y desarrollo de software que describieran el desarrollo, despliegue y mantenimiento» del programa. Este acceso, argumentaba la defensa, era necesario para examinar si el software implementaba correctamente los modelos de genotipificación probabilística y para determinar la fiabilidad de los resultados obtenidos.

Mediante el acceso a esta información la Defensa pretendía poder cuestionar las afirmaciones del Dr. Perlin relativas a la fiabilidad del uso del software de genotipado probabilístico, negándose a aceptar los estudios de validación provistos por la la propia empresa. Respecto a este punto, la Defensa de Pickett subrayó que los estudios de validación presentados por la empresa no cumplían con los estándares exigidos por el *President's Council of Advisors on Science and Technology* (PCAST), ya que ninguno de ellos era independiente ni evaluaba si *TrueAllele* implementó correctamente los métodos estadísticos subyacentes. Según el informe del PCAST, los estudios independientes son esenciales para garantizar que los sistemas de genotipificación probabilística cumplan con estándares científicos robustos y generen resultados confiables. En ausencia de estos estudios, la defensa consideró que aceptar ciegamente los datos proporcionados por la empresa desarrolladora sería incompatible con las garantías procesales.

Asimismo, en respaldo a su postura, la Defensa presentó una declaración escrita por Nathaniel Adams, ingeniero de sistemas contratado como perito de parte. Adams señaló que los cálculos de verosimilitud en *TrueAllele* dependían de modelos estadísticos subyacentes al software, cuya calidad estaba influida y afectaba necesariamente la verosimilitud de los cálculos y, en última instancia, la verosimilitud de los resultados comunicados. Además, destacó que el análisis forense de ADN carece de normas

específicas para el desarrollo y validación de software de genotipificación probabilística, lo que hace indispensable una auditoría exhaustiva del código fuente.

Ante estas presentaciones, Cybergenetics ofreció permitir la inspección del software bajo una «orden de protección» (*protective order*), condicionada a un acuerdo de no divulgación (NDA) dirigido a minimizar la posibilidad de la defensa de argumentar con base al código fuente del sistema *TrueAllele* en juicio público. Sin embargo, la defensa rechazó los términos impuestos, argumentando que las restricciones incluían prohibiciones como tomar notas digitales, acceder a Internet o compilar el código fuente, lo que obstaculizaba una revisión efectiva. Además, se señaló que estas condiciones limitaban la posibilidad de consultas con expertos en áreas relacionadas, como biología, estadística y desarrollo de software, necesarias para evaluar adecuadamente el programa.

Frente a este escenario, la Defensa propuso otra orden de protección que establecía que el material seguiría siendo confidencial y se utilizaría únicamente para preparar la defensa del demandado en este caso. Asimismo se comprometió a que «ningún destinatario podría revelar, utilizar o divulgar ninguna parte». El código fuente se pondría a disposición en un formato accesible especificado en un ordenador autónomo proporcionado por *Cybergenetics* para que el experto lo revisara y, en caso imperioso, «realizara notas de inspección, utilizara el software necesario y creara fragmentos o capturas de pantalla de las líneas de código pertinentes para utilizarlas en su informe». La empresa se negó a aceptar estos términos y se mantuvo firme en sus restricciones al amparo de su derecho al secreto del código fuente del sistema.

b. Contraargumentos de la Fiscalía

Frente a la solicitud de la defensa de acceder al código fuente de *TrueAllele*, la fiscalía presentó una declaración técnica de 78 párrafos elaborada por su testigo experto, el Dr. Mark Perlin. Este documento detallaba los motivos para oponerse a la apertura del código, calificando el pedido como innecesario, irrazonable y contrario al interés de la justicia. Perlin defendió la confiabilidad de *TrueAllele*, destacando su validación dentro de la comunidad científica de genética forense mediante más de treinta estudios y publicaciones.

En su declaración, el Dr. Perlin argumentó que el acceso al código fuente era «inmaterial para el caso», ya que su revisión no aportaría elementos relevantes para determinar la fiabilidad del software. Además, consideró que el análisis del código era impracticable por su complejidad: *TrueAllele* cuenta con aproximadamente 170.000 líneas de código, escritas en MATLAB, un lenguaje de programación matemático especializado en algoritmos numéricos. Según Perlin, descifrar incluso unas pocas líneas de este «denso texto matemático» requeriría un esfuerzo descomunal. Estimó que, al ritmo de diez líneas por hora, una persona tardaría más de ocho años en analizar el código completo.

Sin perjuicio de esta oposición, *Cybergenetics* ofreció al acusado la posibilidad de «inspeccionar» el código fuente bajo un Acuerdo de No Divulgación (NDA). Tras negociaciones extensas, la empresa accedió a flexibilizar algunas condiciones iniciales del NDA, como la entrega de las notas tomadas durante la revisión, pero mantuvo la mayoría de las restricciones. A pesar de estas modificaciones, las partes no lograron un consenso sobre los términos y el alcance de la inspección.

El juez de primera instancia interpretó que la disposición de *Cybergenetics* para permitir un acceso limitado sugería que la principal objeción de la empresa no residía en la entrega

del código en sí, sino en los parámetros que rodearían dicha inspección. No obstante, la defensa sostuvo que incluso los términos revisados seguían siendo excesivamente gravosos y restringían de manera significativa el derecho del acusado a ejercer su defensa.

c. El derecho a la competencia comercial como oposición

Uno de los argumentos más recurrentes presentados por la fiscalía, respaldado por el Dr. Mark Perlin, es la naturaleza del «entorno comercial altamente competitivo» en el que opera *Cybergenetics*. Según Perlin, al menos diez empresas o grupos han desarrollado herramientas similares a *TrueAllele*, como STRmix o FST, lo que subraya la necesidad de preservar la confidencialidad del código fuente. Este planteo se basa en que, en el ámbito comercial, mantener el secreto sobre el código constituye una ventaja estratégica crucial frente a los competidores.

Curiosamente el propio fiscal sostuvo que la revelación del código fuente podría comprometer la posición de *Cybergenetics* en el mercado, dado que las empresas con fines de lucro no suelen poner a disposición del público sus desarrollos tecnológicos. En palabras de Perlin, esta reserva no solo protege los intereses económicos de la empresa, sino que también permite a los desarrolladores mantener un liderazgo en innovación tecnológica frente a rivales en el sector. A su juicio, cualquier apertura indiscriminada del código supondría un daño irreparable para la empresa, otorgando una ventaja indebida a competidores que no comparten la misma información.

Adicionalmente, la defensa de la confidencialidad incluyó la afirmación de que ya se había proporcionado material suficiente para evaluar la fiabilidad del software. Entre los documentos entregados, se destacaron más de treinta estudios de validación y publicaciones científicas que, según la empresa, respaldaban la eficacia y precisión de *TrueAllele*. *Cybergenetics* argumentó que la apertura del código no sólo era innecesaria para el caso, sino que además vulneraba los derechos de propiedad intelectual que le asistían como desarrolladora del software. Por tanto, sostuvo que el material presentado debía considerarse suficiente para cumplir con los estándares judiciales de fiabilidad.

Finalmente, *Cybergenetics* reforzó su posición al señalar que, en un ecosistema donde la innovación tecnológica define el éxito comercial, la divulgación del código fuente representaría no solo una amenaza económica directa, sino también un golpe estructural a las bases competitivas del sector. Según la empresa, ceder en este punto no sólo comprometería sus intereses, sino que también sentaría un precedente peligroso para otros desarrolladores que, ante la posibilidad de verse obligados a exponer sus sistemas internos, podrían optar por abandonar el mercado o limitar sus inversiones en nuevas tecnologías. Así, la competencia comercial no se presenta como un elemento accesorio, sino como el eje principal de su negativa a permitir una inspección irrestricta.

d. Criterio adoptado por el tribunal

Tras analizar los hechos y los planteos de ambas partes, la Suprema Corte de Nueva Jersey se centró en los derechos en conflicto: por un lado, el secreto comercial de *Cybergenetics*; por el otro, el derecho del acusado a preparar una defensa efectiva. El eje de la decisión consistió en determinar si el acceso al código fuente del software *TrueAllele* resultaba indispensable para que la defensa pudiera contrainterrogar al testigo experto para determinar su admisibilidad en el juicio por jurados.

Si bien los jueces reconocieron la importancia de proteger la confidencialidad de los secretos comerciales, dejaron en claro que esta protección no puede prevalecer a costa de obstaculizar el derecho del acusado a una defensa justa. En el considerando V de su decisión, la Corte afirmó que, dado que el Estado había elegido presentar un software novedoso de genotipificación probabilística como prueba y elevarlo al rango de «testigo experto», también debía aceptar un escrutinio exhaustivo del programa. Según los magistrados, una vez que el acusado satisface la carga de demostrar una necesidad particularizada de acceso, el juez debe ordenar la apertura del código fuente y de toda documentación relacionada, como registros de diseño, pruebas, errores, cambios y requisitos técnicos, bajo una orden de protección adecuada.

Este razonamiento convirtió la carga de demostrar la necesidad de acceso en la «llave» para ingresar al análisis interno de un software incorporado al proceso penal. Por ello, la Corte estableció un estándar de cuatro criterios para evaluar si el acusado cumple con este requisito: primero, que exista una base racional para la solicitud, incluyendo el grado en que el testimonio del experto respalda la necesidad de divulgación; segundo, la especificidad de la información requerida; tercero, la existencia de medios disponibles para proteger la propiedad intelectual; y, cuarto, otros factores adicionales relevantes según las particularidades del caso.

En cuanto al primer criterio, la Corte consideró que la defensa presentó argumentos sólidos que justificaban la necesidad de acceso al código fuente. Citó precedentes relevantes, como los casos Chun y Ghigliotty, donde los tribunales reconocieron la importancia del código para validar la confiabilidad de los programas utilizados en procesos judiciales. Además, el tribunal subrayó la contradicción entre el testimonio del Dr. Perlin, quien afirmó que analizar el código llevaría más de ocho años, y la postura de la Fiscalía, que sostenía que las revisiones limitadas ofrecidas por *Cybergenetics* eran suficientes. La Corte resolvió que, aunque la base científica del ADN es válida, esto no garantiza automáticamente la confiabilidad del software que implementa dichos análisis. El código fuente debe ser verificado para garantizar que cumple con lo que *Cybergenetics* afirma.

Respecto al segundo criterio, el tribunal concluyó que la defensa limitó adecuadamente su pedido a la información estrictamente necesaria para una revisión independiente. Argumentó que la divulgación solicitada estaba diseñada para evaluar si el software *TrueAllele* opera según lo previsto y si su funcionamiento no ha sido afectado por errores o modificaciones. La especificidad de la solicitud fue clave para demostrar que el pedido no era arbitrario ni excesivo, sino proporcional a la necesidad de garantizar una defensa efectiva.

En relación con el tercer criterio, los jueces consideraron que las órdenes de protección propuestas por la empresa y la Fiscalía eran excesivamente restrictivas, especialmente por las sanciones automáticas y multas estipuladas en ellas. La Corte señaló que existen otros mecanismos menos gravosos para proteger los secretos comerciales, como sanciones genéricas civiles y penales en caso de incumplimiento. Citó ejemplos de otras jurisdicciones donde las órdenes de protección establecen sanciones proporcionales y genéricas, como suspensiones de licencias o acciones disciplinarias, en lugar de multas automáticas. Instruyó al juez a emitir una nueva orden equilibrada que salvaguarde los derechos de todas las partes y mantenga la jurisdicción necesaria para garantizar su cumplimiento.

Finalmente, en lo relativo al cuarto criterio, la Corte enfatizó que, dado que sistemas como TrueAllele integran disciplinas como informática, estadística y genética forense, su validación requiere un escrutinio multidisciplinario. Aunque el programa sea aceptado en la genética forense, ello no basta si no cuenta con aceptación en otras comunidades científicas relacionadas, especialmente la informática. Este punto es esencial, ya que el escrutinio técnico no debe limitarse a una única disciplina, sino abarcar todas las áreas involucradas en el desarrollo y funcionamiento del software. Esto resalta lo vital que resulta la apertura del código fuente, para así probar que el programa goza también de aceptación dentro de la comunidad informática en general, dentro de la cual también opera y se desarrolla.

En conclusión, la Corte consideró que la defensa cumplió con los cuatro requisitos establecidos para acceder al código fuente y demás información complementaria.

En el considerando VI, subrayó que, a medida que avanza la tecnología, los jueces deberán ejercer un «sano escepticismo» al evaluar herramientas novedosas en procesos penales, asegurando una defensa efectiva para los acusados. Recordó que los programas informáticos, al ser diseñados por humanos, están sujetos a errores, defectos y sesgos. Por ello, solo una revisión independiente y sin restricciones puede garantizar su confiabilidad bajo estándares como Frye o Daubert. Finalmente, la Corte ordenó revertir el fallo apelado y remitir el caso, instruyendo al juez a compeler la divulgación del código fuente y la documentación relacionada. Además, ordenó que el juez supervise el cumplimiento de la orden de protección y actúe como garante de un escrutinio efectivo en el marco de la audiencia bajo el estándar *Frye*.

8. Impacto y reflexiones

El caso *State v. Pickett* permite reflexionar respecto a un aspecto que ha adquirido una relevancia creciente para el derecho procesal: la relación e interacción entre la tecnología de uso judicial y la vigencia de las garantías procesales. La digitalización del sistema judicial y la incorporación de diverso tipos de herramientas algorítmicas transforman el modo en que se recolectan y valoran las pruebas, planteando nuevos desafíos y tensiones frente a determinados pilares perentorios del proceso como son la publicidad de los actos procesales, la igualdad de armas y el control de los medios probatorios. Si bien la modernización de la justicia es un fenómeno inevitable, no siempre queda claro hasta qué punto estos avances tecnológicos son compatibles con los principios que estructuran el proceso penal.

El problema que subyace en este caso no se reduce a la fiabilidad técnica de *TrueAllele* ni a su reconocimiento dentro de la comunidad forense, sino a una cuestión más amplia: la posibilidad de controlar y contradecir los medios de prueba presentados en juicio. En los sistemas acusatorios, la prueba no adquiere validez por su sola existencia, sino por su capacidad de ser sometida a debate y verificación. La pregunta que surge, entonces, es si puede considerarse plenamente válida una prueba cuyo funcionamiento interno no es accesible para las partes ni para el tribunal. La Corte de Nueva Jersey ha dado una respuesta afirmativa en este caso, al establecer que la defensa tenía derecho a conocer el código fuente del software utilizado en su contra. Sin embargo, la cuestión no está resuelta en términos generales y es probable que este tipo de debates continúe profundizándose en los próximos años.

Más allá de la solución concreta adoptada en este caso, la discusión refleja una tensión que va en aumento: el papel que deben tener las tecnologías privativas en la producción de prueba penal. La exclusión de la defensa y del tribunal en la evaluación de la estructura interna de estos sistemas genera un desequilibrio que es difícil de justificar en términos procesales. El derecho de defensa supone la posibilidad real de contraexaminar la prueba presentada en juicio, pero ¿Cómo se materializa este derecho cuando los fundamentos del análisis probatorio no pueden ser revisados? La respuesta no es sencilla, pero el problema no puede reducirse únicamente a una cuestión de conveniencia o de eficiencia en la administración de justicia.

Este caso también pone de relieve otro aspecto que no puede ser soslayado: la introducción de actores privados en la producción de prueba penal. A diferencia de los métodos tradicionales de evaluación pericial, que en su mayoría son llevados a cabo por organismos públicos, universidades o laboratorios forenses estatales, el uso de software privativo implica delegar una función judicial clave en empresas que operan bajo una lógica comercial. Esto introduce un problema estructural, ya que el diseño y la implementación de estos sistemas responden a intereses de mercado que pueden entrar en tensión con las exigencias de imparcialidad, publicidad y control que rigen el proceso penal.

El caso aquí analizado muestra con claridad esta problemática. La negativa de *Cybergenetics* a revelar el código fuente de *TrueAllele* no se debió a razones técnicas ni científicas, sino a la necesidad de proteger su propiedad intelectual y su modelo de negocios. En otras palabras, el software no se presentó como una herramienta de conocimiento abierto y replicable, sino como un producto comercial cuyo funcionamiento debía mantenerse en secreto. Esto plantea una cuestión central: ¿Es compatible con los principios del proceso penal la introducción de tecnologías cuyo control efectivo se encuentra limitado por estrategias de mercado? La preocupación no es menor, ya que aceptar este modelo sin restricciones podría derivar en un escenario en el que la prueba digital se convierta en un insumo privatizado, cuyo acceso dependa de acuerdos comerciales entre el Estado y las empresas desarrolladoras.

Este punto adquiere aún mayor relevancia en la medida en que los sistemas de justicia comienzan a integrar herramientas de inteligencia artificial para la toma de decisiones. Modelos predictivos para evaluar la reincidencia, sistemas de reconocimiento facial para la identificación de sospechosos y algoritmos para la determinación de penas son solo algunas de las aplicaciones que han comenzado a desarrollarse. No obstante, el uso de estas herramientas plantea interrogantes sobre su impacto en los derechos fundamentales. La tendencia hacia la automatización de la justicia podría generar una ilusión de objetividad, cuando en realidad estos sistemas operan a partir de modelos construidos por humanos, con sus propios sesgos y limitaciones. En este escenario, la exigencia de publicidad de los actos procesales adquiere una dimensión aún más relevante, pues sin la posibilidad de examinar y cuestionar los métodos utilizados, la presunción de imparcialidad y confiabilidad de estas tecnologías no es suficiente para garantizar su legitimidad.

El avance de la inteligencia artificial y los sistemas algorítmicos en el derecho penal plantea un desafío que no puede reducirse a una cuestión de eficiencia o rapidez en el procesamiento de información. La creciente centralidad de estas herramientas en el desenvolvimiento del proceso exige que su implementación se haga bajo criterios que aseguren su plena compatibilidad con las garantías constitucionales. No se trata únicamente de regular su uso, sino de definir con precisión qué condiciones deben

cumplirse para que su aplicación en el proceso penal no genere desigualdades estructurales ni debilite el derecho de defensa. El problema no radica en la incorporación de tecnología en la justicia, sino en permitir que estas herramientas operen bajo esquemas opacos o con limitaciones que impidan su control efectivo. Sin estándares claros que regulen su diseño y uso, el riesgo no es solo la consolidación de mecanismos de prueba de difícil impugnación, sino la progresiva erosión de los principios que sostienen la legitimidad del proceso.

El debate abierto por este fallo no se agotará en la cuestión específica de *TrueAllele* ni en el problema del acceso al código fuente. Más bien, constituye un punto de partida para repensar cómo debe estructurarse la relación entre derecho y tecnología en los procesos judiciales. La modernización de la justicia no puede interpretarse como un simple proceso de incorporación de nuevas herramientas, sino como un desafío que obliga a evaluar continua y críticamente el impacto de estas innovaciones en la forma en que se administra la prueba, se garantizan los derechos y se equilibra el poder entre las partes. Lo que está en juego no es solo la publicidad de un software en particular, sino el sentido mismo de la contradicción y del control de la prueba en el sistema penal.

Casos como este trazan una línea clara sobre cómo debe pensarse la integración de tecnología en el derecho procesal penal, no solo desde el análisis de su impacto en las garantías individuales, sino también desde su diseño e implementación en la esfera pública. Resulta imperativo que los Consejos de la Magistratura elaboren planes de contratación pública de tecnología desarrolladas específicamente para la particular función de impartir justicia. La adquisición y desarrollo de software con impacto procesal no puede ser regulada bajo los mismos parámetros que para los servicios comerciales, sino que debe responder a criterios específicos que garanticen el respeto irrestricto de las garantías constitucionales para, así, respetar los principios que estructuran el proceso y evitar nulidades. Esto implica garantizar la explicabilidad de los sistemas o, en su defecto, la adopción de estándares de auditoría independientes, asegurando que las herramientas utilizadas en el proceso penal no introduzcan restricciones que vulneren el derecho de defensa ni comprometan la imparcialidad de las decisiones judiciales. La tecnología puede aportar mucho al derecho penal, pero su integración debe realizarse con pleno respeto a los principios que rigen el proceso, asegurando que las herramientas del futuro se diseñen no sólo para ser eficientes, sino, ante todo, para ser justas.

9. Bibliografía

Busaniche, B. (s.f.). *El dilema del copyright en el campo del software*. Fundación Vía Libre. https://vialibre.org.ar

Capellino, A. (2024). 10 de junio. The Frye Standard in Expert Testimony. *Expert Institute.*

https://www.expertinstitute.com/resources/insights/admitting-expert-testimony-under-the-frye-standard-the-ultimate-guide/

Culebro Juárez, M., Gómez Herrera, W. G., & Torres Sánchez, S. (2006, mayo). *Software libre vs software propietario: Ventajas y desventajas*. Creative Commons.

Giostra, G. (1989). *Processo penale e informazione* (2ª ed.). Giuffrè.

Kirchner, L. (2017). Thousands of Criminal Cases in New York Relied on Disputed DNA Testing Techniques. *ProPublica,* 4 de septiembre.

https://www.propublica.org/article/thousands-of-criminal-cases-in-new-york-relied-on-disputed-dna-testing-techniques

Morozov, E. (2016). *La locura del solucionismo tecnológico*. Katz.

Pomar, T. F. (2022, marzo 16). Acceso a la información pública y software: Hacia la plena publicidad de los códigos fuente empleados por el Estado. *Revista Pensamiento Penal*.

Pomar, T. F. (2023). *Algoritmos judiciales, un nuevo velo de la justicia.* En *Garantizando la independencia de la justicia: El papel del Consejo de la Magistratura* (Dossier). Buenos Aires: ADC.

Jurisprudencia:

Pennsylvania Superior Court, «*Kevin James Foley*», 2012. 38 A.3d 882, 889–890.

Crown Court (UK), «*Colin Pitchfork*», 1988.

State of New Jersey, «*Corey Pickett*», Exp. No. A-4207-19T4 (págs. 14, 15 in fine, 16, 16–17, 18, 18 in fine, 21, 21 in fine).

United States Supreme Court (USSC), «*Brady v. Maryland*», 1963.