

PROBLEMÁTICA DE LOS *DEEPFAKES* COMO RESULTADO DE LAS DILIGENCIAS INICIALES DE INVESTIGACIÓN EN LA JURISDICCIÓN PENAL SALVADOREÑA.

CARLOS ENRIQUE QUINTANILLA CHÁVEZ

1. INTRODUCCIÓN

Históricamente, primero acontece el comportamiento social y luego aparece el Derecho para regularlo, casi siempre a velocidades diferentes. El jurista y ex Ministro de Justicia de Prusia, Friedrich Karl von Savigny; ya desde mediados del siglo XIX sostenía que “el Derecho se encuentra en el espíritu del pueblo”¹ al que denominaba *volksgeist*. Nada ha cambiado en la actualidad, pues, como otros actores más contemporáneos apuntan, el Derecho siempre va detrás de la sociedad². Con la llegada de la cuarta revolución industrial, así llamada por Klaus Schwab, los avances tecnológicos han venido a dar un giro transformador en el diario vivir de las personas, en donde el derecho no escapa a estas modificaciones.

Por lo anterior, el presente trabajo pretende identificar los retos que plantea la inteligencia artificial (en adelante IA) al proceso penal y, en particular, los denominados *Deepfakes* obtenidos en las diligencias iniciales de investigación, mismos que, a pesar de ser falsos, cuentan con la capacidad de servir como fundamento para la toma de eventuales decisiones administrativas o judiciales injustas.

Finalmente, se proponen alternativas encaminadas a prevenir que las evidencias digitales falsas puedan contribuir con la vulneración a derechos y garantías fundamentales de las partes procesales, haciendo especial énfasis en la prueba pericial.

2. LA INTELIGENCIA ARTIFICIAL Y SU ENTORNO SOCIAL ACTUAL

Tanto el cerebro humano, como su funcionamiento, han conformado gran parte de la ambición tecnológica que pretende descifrarlo a base de estudios multidisciplinarios, aplicando las neurociencias, psicología, neurología e ingeniería. Entre sus alcances se encuentra la IA, término acuñado por John McCarty, a quien se le atribuye el título de Padre de la inteligencia artificial, concepto al que arribó en 1956 debido a que creía que una computadora podría simular la forma de pensar del ser humano³.

¹ SAVIGNY, K.F.: *Los fundamentos de la ciencia jurídica*. Ediciones Olejnik.

² OTERO LASTRES, M.; *El derecho siempre va detrás de la sociedad, debe adaptarse a la realidad en que se vive. La Opinión A Coruña*.

³ DATASCIENTEST: *Todo sobre John McCarthy*, s.l., s.f.

No cabe duda de que, con fundamento en algoritmos y modelos matemáticos, la IA es capaz de tomar decisiones derivadas de patrones y reglas de aprendizaje automático y constante, convirtiéndola en aquella pensada herramienta parecida al cerebro humano que, por más controversial, terminó por ser —y continúa siéndolo— uno de los temas más significativos del siglo XXI, más cuando las personas parecen estar interesadas en alcanzar todo a la vuelta de la esquina⁴. Estos sistemas informáticos de IA pueden pensar como humanos, actuar como humanos, pensar racionalmente y actuar racionalmente⁵.

Lo antes mencionado indica que la IA, sea por software o por inteligencia artificial integrada, ofrece a la humanidad asistentes personales digitales, el internet de las cosas, vehículos autónomos, marketing digital, búsquedas en la web, optimización de productos, procesos de ventas, reconocimiento de voz y rostro, robots, drones y demás, tal cual lo describe el Parlamento Europeo en su portal de información, entidad que, a su vez, sostiene que la IA posee la habilidad de prestar las mismas capacidades que los seres humanos, así se trate del razonamiento, aprendizaje, creatividad y capacidad de planear⁶.

Con tales características, la IA se ha difundido, enrolado y consolidado, de manera generalizada, con una popularidad alarmante; de hecho, ha superado las expectativas. Diversos expertos aseguran que se ha integrado en la vida de las personas de tal manera que, para mediados de febrero de 2025, por ejemplo, ChatGPT, con todo y sus errores, alcanzó 400 millones de usuarios activos⁷.

Se enfatiza que, el uso de la IA ha adquirido una novedosa dinámica de acceso a la información, convivencia, socialización, forma de educación, contribución en la medicina y en muchas otras áreas. De acuerdo a expertos de la Universidad Internacional de Valencia, la estructura, acceso y resultados de estos sistemas, un tanto diferentes a los que veníamos acostumbrados, ha superado antiguos paradigmas, permitiendo la automatización de procesos, reducir el error humano, potenciar la creatividad, agilizar la toma de decisiones, analizar errores de seguridad, aportar precisión, generar avances en el sector salud, etc.; pero, al mismo tiempo, puede servir como instrumento para causar la vulneración de derechos, dificultar el acceso a datos, generar pérdida de empleos, entre otros⁸.

Es de señalar ciertos esfuerzos regulatorios orientados a prevenir el impacto negativo de estos sistemas, por ejemplo, la Unión Europea y el Reglamento de la IA (2024), que promueve la protección de derechos y libertades de usuarios, normas de aplicación a

⁴ SALAZAR C., A.: “La inteligencia artificial vs la inteligencia humana”, Duazary, vol. 15, n.º 3 (2018), p. 249

⁵ RUSSELL, S. y NORVIG, P.: *Artificial Intelligence: A Modern Approach*, 4.ª ed., Upper Saddle River, NJ, Pearson, 2021.

⁶ PARLAMENTO EUROPEO: *¿Qué es la inteligencia artificial y cómo se usa?*, 27 de agosto de 2020.

⁷ INFOBAE: *ChatGPT tuvo mayor popularidad con el anuncio de nuevos lanzamientos y ya cuenta con 400 millones de usuarios*, 7 de marzo de 2025.

⁸ UNIVERSIDAD INTERNACIONAL DE VALENCIA: *Inteligencia artificial, ventajas y desventajas*, 5 de marzo de 2024.

proveedores de IA, el enfoque basado en riesgos, la ética, sugiere prohibiciones generales, vigilancia y recomienda que sea una persona física o jurídica la que debería responder por un sistema de IA que no se adapte a las exigencias reguladas⁹. También el abordaje superficial realizado por la Ley de Fomento a IA y Tecnologías en El Salvador (2024)¹⁰. Ambos cuerpos normativos que pretenden establecer las reglas de introducción de sistemas basados en IA generativas, sin la capacidad de controlar la ruta probatoria que resuelva fácticos como los que aquí se abordarán.

3. INTELIGENCIA ARTIFICIAL Y DERECHO

La inteligencia artificial ha provocado un “cambio de ritmo social” que, sin duda, también trae su consecuencia en el quehacer judicial. Y no es casualidad. Más allá de las vivencias colectivas, esta circunstancia viene a situar al sistema de justicia en un escenario sin precedentes. Debe recordarse que, la sociedad concibe a los tribunales como el lugar donde se imparte justicia. De hecho, la potestad de juzgar y hacer ejecutar lo juzgado corresponde al Órgano Judicial (Artículo 172 inc. 1º de la Constitución de la República de El Salvador y 117 párrafo 3º de la Constitución Española).

Sin embargo, esto de juzgar y hacer ejecutar lo juzgado vive una batalla constante con la percepción y realidad de la población. El trabajo realizado por la Unión Europea concluyó que, en marzo de 2023, el 79% de los europeos consideraron que las tecnologías digitales serán importantes en sus vidas para el 2030¹¹ y, por otra parte, el Centro de Investigaciones Sociológicas arrojó que en 2024 las personas valoraron con un 4,67 el nivel de confianza que les genera la justicia¹². Con esto, la invitación a ser protagonistas con el propósito de mejorar la calidad de la justicia.

Por obvias y lógicas razones, el juzgamiento en épocas de inteligencia artificial requiere un especial interés, pero no enfocado en el impacto estos sistemas en la administración de justicia como herramienta de agilización de procesos (documental y de gestión), tampoco de sistemas expertos jurídicos (SEJ), mismo que fue ideado por Andrew Stranieri¹³, sino desde la óptica eminentemente procesal, relacionado con aquellos *Deepfakes* que pretendan servir al proceso penal como resultado de las diligencias iniciales de investigación.

⁹ UNIÓN EUROPEA: *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial...*, Diario Oficial de la Unión Europea, 2024.

¹⁰ ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR: *Ley de fomento a la inteligencia artificial y tecnologías*, 2024.

¹¹ COMISIÓN EUROPEA: *Eurobarómetro especial 518 – Actitudes hacia el impacto de la inteligencia artificial y la robótica*, 2023.

¹² CENTRO DE INVESTIGACIONES SOCIOLÓGICAS (CIS): *Barómetro de marzo 2024. Avance de resultados*, 2024.

¹³ CORTE INTERAMERICANA DE DERECHOS HUMANOS: *Opinión Consultiva OC-24/17: Medio ambiente y derechos humanos*, 7 de febrero de 2018

3.1.Una sentencia londinense

No era necesario dejar pasar tanto tiempo para que el sistema judicial se viera involucrado en la complejidad que conlleva la posibilidad que la IA genere *Deepfakes*. Recientemente, el 6 de junio de 2025 para precisar, un Tribunal Divisional con sede en Londres, en relación a la competencia y conducta de abogados, ha tenido que resolver en relación a “...*the actual or suspected use by lawyers of generative artificial intelligence tools to produce written legal arguments or witness statements which are not then checked...*”¹⁴.

Brevemente, trata de dos casos acumulados. El primero, donde una abogada habría tergiversado lo dispuesto en la Ley y relacionada jurisprudencia de casos inexistentes. Aunque no se demostró probatoriamente el uso de IA para su obtención, el tribunal aseguró que había intencionalidad y con ello pretender engañar. La abogada, reconoció su negligencia y dijo que nunca pretendió engañar al tribunal. El tribunal supuso la existencia únicamente de dos posibilidades, una, que deliberadamente se realizaron las citas falsas, y dos, haber utilizado herramientas de IA generativa; en una u otra se estaría siempre ante información falsa y, por tanto, desacato.

El segundo, tanto el cliente como su abogado agregaron en sus declaraciones 45 citas y las presentaron ante el tribunal. De estas, 18 no existían y el resto no contenían las citas atribuidas a cada caso. El demandante reconoció que las citas fueron generadas por la IA, motores de búsqueda legales y fuentes en línea, pero que no pretendía tergiversar la ley ni causar confusión al tribunal, pidiendo que exoneraran a su apoderado por haberlo inducido a error. El abogado, por su parte, admite haberse basado en la investigación realizada por su representado sin haberla verificado sin la intención de engañar al tribunal. Se concluyó que el abogado no tenía la intención de engañar, pero enfatizó en la conducta, exclamando que al profesional no debió confiar en su cliente.

En ambos casos, la decisión final fue la de no iniciar un procedimiento por desacato, pero los abogados fueron remitidos a la Autoridad Reguladora de Abogados.

Esta experiencia expone la vulnerabilidad de los procesos en relación a los *Deepfakes* y que, en casos concretos, la evidencia puede ser excluida por falsa, pero no se sigue el tratamiento penal por las acciones falsarias o defraudatorias del proceso. Por cierto, en otros precedentes se ha sostenido que no se puede proceder contra el abogado por desacato debido a que, según el estándar de prueba penal, no se puede asegurar que sabía que las citas eran falsas¹⁵, denotando incertidumbre si se tuviera que proceder penalmente.

Es muy interesante que, esta sentencia no cuenta con razonamientos que permitan responder, por ejemplo, cuál fue el procedimiento utilizado por la autoridad para determinar

¹⁴ HIGH COURT OF JUSTICE (UK): *Ayinde v. London Borough of Haringey and Al-Haroun v. Qatar National Bank*, Sentencia de 6 de junio de 2025.

¹⁵ HIGH COURT OF JUSTICE (UK): *Olsen v. Finansiell Stabilitet AS*, Sentencia de 16 de enero de 2025.

que las citas eran falsas o cómo concluyó que se trataba de IA o con qué elementos contó para determinar posibles responsabilidades profesionales. A todas luces, casos como éste, implican un desafío técnico, jurídico y procesal, pero se debe ir más allá, pensando por ejemplo en *Fake You*, *DeepArt*, *Cap Cut*, *Chatbots* y otros que, con su capacidad de crear, producir, recrear, alterar, simular y representar escenarios aparentemente reales, podrían plantear serios problemas.

3.2. Tratamiento de la evidencia digital

El Salvador regula la evidencia digital en el Art. 259-A del Código Procesal Penal, la que será admisible como prueba y deberá valorarse de conformidad a las reglas de la sana crítica. Ahora bien, ¿será que al momento en que el legislador la incluyó pensó en que ésta podía ser falsa o verdadera?

Basta con conocer que, según sus considerandos, la evidencia digital será admisible aduciendo que en ésta quedan “rastros” del cometimiento de delitos y que por medio de ella es posible detectar, investigar y sancionar delitos¹⁶. De hecho, cuando esta disposición se refiere a la autenticidad, nunca advierte la posibilidad de *Deepfakes* y, exclusivamente, exige que sea demostrable la “acreditación de autenticidad”, misma que podrá surgir por: i) por el testimonio de quien intervino directamente en la elaboración, generación, transmisión o recepción de la evidencia digital; ii) por la acreditación de los mecanismos técnicos informáticos utilizados para su generación; y iii) por un perito que haya intervenido en su obtención, resguardo o almacenamiento.

Dicho esto, no fue pensada incluyendo la posibilidad de *Deepfakes*. Se sigue profesando una especie de “confianza informática”, suponiendo que la evidencia digital es pura y sagrada, incapaz de revelar información falsa.

Bajo este argumento, la alternativa probatoria idónea es la extracción de información o vaciado de información, en donde el experto parte de la existencia de un dispositivo electrónico, para luego determinar la obtención o transmisión de información. Pero es el dispositivo y el contenido son dos mundos diferentes.

La pericia informática, dentro de sus áreas de estudio, incluye el “análisis de la información”, donde el experto en informática emite sus valoraciones técnicas de lo observado a través de la extracción. Visto esto, ¿cuál sería el resultado de llevarle un *Deepfake*? Claro está, con la creatividad generativa de la IA, debe dejar de pensarse que el contenido de la información es indiscutiblemente verdadero.

4. INMINENTE PERJUICIO PROCESAL DE LOS *DEEPFAKES*

En fin, la prueba tiene por objeto llevar al conocimiento del juez o tribunal los hechos y circunstancias objeto del juicio, especialmente en lo relativo a la responsabilidad penal y

¹⁶ REPÚBLICA DE EL SALVADOR: *Decreto Legislativo n.º 280, de 1 de febrero de 2022, Considerandos IV y V.*

civil derivada de los mismos, así como, conseguir la convicción del juzgador sobre la realidad de los hechos¹⁷. Misma que se aplica indudablemente a la naturaleza de los resultados de las diligencias iniciales de investigación. Lo fundamental es que el litigante pueda aportar evidencias que justifiquen lo que dice, trayendo al proceso la realidad acaecida fuera del mismo¹⁸. Evidentemente, al referirse a los “hechos”, pretende su enfoque en “hechos verdaderos”, se insiste, “no en hechos falsos”, los que estarán a cargo de la parte que los pretende hacer valer. Eso sí, sin apartarse del principio de legalidad, utilidad, necesidad y pertinencia.

El proceso penal y el tratamiento de la evidencia poseen sus propias características, adecuadas que sean para los efectos del presente trabajo en aquellos elementos que puedan resultar de las diligencias iniciales de investigación con forma de indicios o elementos de convicción, los cuales, una vez recogidos, son administrados en sede administrativa fiscal y policial en forma unilateral, sirviendo oportunamente para el ejercicio de la acción penal, aunque con posterioridad puedan alcanzar la categoría de pruebas en el proceso. En tal calidad, éstos poseen la capacidad de servir de fundamento para: a) definir la categoría de sobreaveriguar de una investigación; b) atribuir la calidad de víctimas, imputados y responsables civiles; c) emitir órdenes de captura; y d) judicializar procesos penales.

Objetivamente, sea que se esté ante diligencias iniciales de investigación o pruebas, éstas informan al proceso, significando que, aun con anterioridad al juicio oral, poseen el potencial de ser utilizadas como fundamento para la toma de decisiones, incluso sin oportunidad de contradicción. Mírese el caso de la orden de captura o en el tratamiento de reos ausentes. No obstante, a pesar de catalogarse como meros elementos indiciarios o diligencias iniciales de investigación, pueden justificar el mantenimiento, modificación o revocación de resoluciones. Verbigracia, la apariencia de buen derecho, relacionada con la existencia del delito y la autoría o participación delincuenciales. Por tanto, aquí se enaltece el alcance de éstos y sus consecuencias procesales significativas.

Visto lo hasta aquí apuntado, es irrefutable que las pruebas son las únicas que el legislador dispuso con la posibilidad de demostrar aspectos relacionados con el fondo del asunto y que la presunción de inocencia puede vencerse únicamente por medio de éstas; a pesar de ello, y sin llegar a la implicancia de una condena o de la absolución, el proceso penal permite que con los elementos y hallazgos producidos en las diligencias iniciales de investigación sea posible afectar, restringir o modificar el ejercicio de derechos y garantías fundamentales, sea desde el inicio de la investigación, hasta la incoación del proceso o, desde atribuir la calidad de investigado, hasta la imposición de medidas cautelares o precautorias (Arts. 75, 270 y 271 C. Pr. Pn.).

¹⁷ PUERTA LUIS, L.R.: *La prueba en el proceso penal*, s.l., s.f.

¹⁸ NIEVA FENOLL, J.: *Teoría General del Proceso (Derecho Procesal I)*, Valencia, Tirant lo Blanch, s.f., p. 138.

A todas luces, verificar la importancia y trascendencia de estas categorías-evidencias se hace con el afán de identificar la ausencia de un pseudo-contradictorio u oportunidad de contradicción como consecuencia del descubrimiento de *Deepfakes*, pero que, aun con la oportunidad que pueda tener el perjudicado para rebatir el dato falso, no implica que imperiosamente le sea tan posible.

Imagínese a una persona que aduce ser víctima de delito y, para sostenerlo, exhibe un archivo de audio en el que consta el intercambio de conversaciones entre ella y el presunto hechor, de donde supuestamente se deriva, por ejemplo, una amenaza de muerte. En un supuesto como éste, sin olvidar la mal llamada presunción de buena fe, en el supuesto de considerarse útil la información digital y tras recoger otras diligencias menos tecnológicas, muy probablemente, con o sin extracción y análisis de la información, permitirá iniciar una investigación, se calificará el probable delito, designarán la calidad de víctima, se individualizará al probable responsable y en su momento se judicializará. De igual manera, pero con menos filtros, será en caso de flagrante delito.

Es evidente que los elementos indiciarios o diligencias iniciales de investigación pueden dar lugar al inicio del proceso penal. Ahora bien, ¿cuál es la oportunidad con la que cuenta el perjudicado, desde un enfoque garantista actual, si se tratase de un *Deepfake* creado por la supuesta víctima a través de la inteligencia artificial generativa? ¿Será cierto que, durante etapas tempranas administrativo-judiciales existe una verdadera oportunidad procesal para refutarlo?

Con cara de laguna, pero con cuerpo de mar, en tiempos de los *Deepfakes*, aquí se halla plenamente identificado un defecto procesal que implica la posibilidad de vulnerar potencialmente derechos y garantías fundamentales¹⁹. Dilucidense al menos dos problemáticas, la primera, relacionada con el libertinaje falsario y, la segunda, con la inviabilidad procesal de contrarrestar el poder de una evidencia digital falsa.

Cruelmente cabe señalar que ya se dedica tiempo significativo con la intención de superar y sobreponerse a las flagrantes adversidades sufridas por la presunción de inocencia²⁰ y de lograr calidad en la fundamentación de las sentencias²¹, como para ver afectado al proceso penal con un flagelo adicional, relacionado con el eminente riesgo de la iniciación o seguimiento de la investigación penal con origen en *Deepfakes*.

¹⁹ RUVALCABA GÓMEZ, C. y PADILLA PADILLA, R.: “Repensando los Derechos Humanos en tiempos de Inteligencia Artificial”, en: *Inteligencia Artificial y Derechos Humanos: debate actual y de futuro*, Tomo V, Valencia, Tirant lo Blanch, s.f., p. 178.

²⁰ NIEVA-FENOLL, J.: *La razón de ser de la presunción de inocencia*. InDret Revista para el Análisis del Derecho.

²¹ COLOMA CORREA, R., PINO YANCOVIC, M., Y MONTECINOS SANHUEVA, C.: “Fundamentación de sentencias judiciales y atribución de calidad epistémica a las declaraciones de testigos en materia procesal penal”. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, n.º XXXIII.

5. ¿CÓMO Oponerse a los *Deepfakes*? UNA PROBLEMÁTICA PROCESAL

Inicialmente cabe señalar que los *Deepfakes*, derivados del proceso de generación por la vía del aprendizaje profundo y automático de inteligencia artificial, denominados “ultrafalsificación”²², son los que constituyen el objeto principal de este estudio, a consecuencia de la capacidad que tienen de producir una sensación de autenticidad o veracidad aun siendo falsos.

Procesalmente, es idóneo destacar dos eventuales supuestos, primero, la posibilidad de valerse de un *Deepfake* para demostrar que, con él, se ha cometido un hecho tipificado como delito y, otro muy diferente es pretender engañar la investigación o al juez por medio del mismo. Parece sencilla la diferencia, no obstante ser falsa la evidencia en ambos escenarios. Curiosamente, en el primer enunciado, el *Deepfake* podría ser válido y admitido, circunstancia en la que hoy no se profundizará, empero, en el segundo, estará sujeto a inmediata exclusión, so pena de las responsabilidades que puedan surgir de su uso, tal cual el caso londinense.

Sin enredar más el asunto, ahora no se va a hacer referencia a la valoración de la prueba, que procesalmente propone un escenario más tardío. Como se dijo, interesan aquí las fases previas. Y no se pretende hacer caso omiso a que, conforme a la experiencia y por mandato del legislador, es hasta en el juicio oral el momento en que se realizará tal valoración, salvo excepciones.

Es válido afirmar que, con relación a las instituciones públicas, ha prevalecido la buena fe, en el particular, ejercida por los usuarios del sistema de justicia, sea por costumbre, educación, institucionalidad o simplemente por el conocimiento que se posea de las consecuencias legales por su infracción. También es cierto que, las herramientas informáticas, hasta hace no muchos años, no facilitaban a la población en general la posibilidad de crear *Deepfakes*, proliferados de forma desmesurada con su llegada y popularidad.

¿Es posible ejercer un legítimo y verdadero derecho de contraprobanza oponiéndose a las intenciones perjudiciales de los *Deepfakes* en las referidas y prematuras fases procesales? Se adelanta desde ya que, irónicamente, aun tratándose del juicio oral, probablemente el defecto, por el momento, se mantendría vigente.

Para dar respuesta a la interrogante, se inicia por identificar dos momentos, uno, donde el *Deepfake* no es conocido por su perjudicado y otro en el que sí. Delimitados así con el objeto de evaluar la existencia o no de oportunidades procesales idóneas para su oposición.

En una primera realidad posible, el Ministerio Público Fiscal, al recibir la evidencia, muy probablemente atenderá a la versión proporcionada por el informante, derivado que sea

²² BLÁZQUEZ MORENO, R.: “*Deepfakes en el procedimiento probatorio*”, A Coruña, s.l., s.f., p. 226.

de una posible denuncia o entrevista. Con suerte, habrá elementos de corroboración como simples documentos impresos que ilustren el contenido digital. Lamentablemente, ninguno de ellos tendrá la capacidad objetiva, ni científica, para acreditar la veracidad del contenido de la información digital. Es improbable que, existiendo voluntad maliciosa, el que dirige la investigación pueda descubrir la falsedad del *Deepfake*, menos aún, que realice las diligencias pertinentes para su comprobación.

Suponiendo que el afectado se entera de la existencia del *Deepfake* que opera en su contra, lo predecible es que intentará oponerse con la especial esperanza de rebatirlo. Pero ¿cómo será esto? Un simple alegato de objeción a la evidencia falsa no bastará, peor en el caso de ser el investigado, por más que insista en que el contenido no coincide con la realidad y pretenda invocar la existencia de sistemas de inteligencia artificial generativa que permiten la producción o creación de *Deepfakes*. Tampoco es acertado decir que existe la oportunidad plausible de requerir o encomendar la realización de una prueba o diligencia específica que tenga la capacidad de contrarrestar objetivamente la autenticidad del contenido falso de éstos.

En teoría, por su carácter técnico o científico²³, la única alternativa viable y objetiva sería la pericial, con la que se debe tener especial cautela, debido a que, hasta hoy, han tenido como propósito la determinación de la autenticidad de la información únicamente por su origen y no por el contenido como tal.

Pero aquí ocurre que, una cosa es determinar la fuente, soporte y falta de alteración, y otra muy diferente es acreditar la veracidad del contenido en sí mismo. Significativamente, se exhorta diferenciar dos misiones del peritaje, por un lado, determinar el dispositivo por medio del cual se produce la extracción y, por otro, la propia prueba en sí. Separar el continente del contenido. Equivocadamente se supone que, una vez sentadas las bases de autenticidad del dispositivo el contenido es verdadero.

Respecto a los *Deepfakes*, al practicar la pericia informática orientada únicamente en la autenticidad del dispositivo, confirmaría la autenticidad de su continente, pues existe un dispositivo de origen, contiene la información y no posee alteraciones; es decir, el soporte informático existe, el archivo se encuentra en su interior y no ha sido manipulado. En conclusión, la premisa relacionada con la autenticidad, de nada sirve al momento de discutir el carácter de “falso” del contenido. Visualícese a la contraparte valiéndose del resultado de la pericial propuesta por el mismo desfavorecido de la evidencia falsa.

Someramente, es correcto pensar que la respuesta sí que se encuentra en la pericial, aunque actualmente no sea posible requerirse ante los equipos o entes encargados de la práctica científico-forense institucional, ni particular. Se dice así a razón que no existe actualmente la posibilidad de demostrar científicamente que una evidencia sea *Deepfake*. Llama la atención la postura de alguien por ahí que asegura la posibilidad de contrarrestarlos

²³ “La prueba pericial. Consideraciones sobre la prueba pericial y su valoración en la decisión judicial”, REDEA – Derechos en Acción, año 2, n.º 4, Invierno 2017, p. 131

por medio de lo que denomina “técnicas” para identificar representaciones sintéticas, con base al análisis de metadatos, filtrado de color, número de parpadeos, cuerpo en escena, ruido, coordinación del sonido con los labios, superposición de imágenes y otros que, dejando a criterio de los expertos su utilización en la práctica forense²⁴.

Es un tanto curioso pretender asimilar que un sistema informático de IA, dotado de una significativa cantidad de sesgos, pueda ser la herramienta idónea para la detección de *Deepfakes*, lo cual no significa que sea imposible. Tal cual lo sostiene Jesús Punzón Moraleda, los sesgos “pueden surgir tanto en procesos algorítmicos como en la toma de decisiones humanas”²⁵, el problema es que esos sesgos discriminadores pueden producirse por diversas puertas de entrada y pueden no ser fáciles de apreciar²⁶, refiriéndose al inadecuado entrenamiento de los algoritmos y su selección.

En tal sentido, con todo esto de los algoritmos, sesgos y, en fin, de la inteligencia artificial ¿será posible pensar en que la falsedad de los *Deepfakes* será comprobada por medio de sistemas que no han superado el estándar de la prueba pericial? Ante esta paradoja, la pericial informática incurriría en un disparate al que se le puede denominar “la aplicación de los criterios *Daubert* al revés”; tal cual se tratase de una verdadera carga de la prueba para el perjudicado por los *Deepfakes*. Aquel desarrollo jurisprudencial estadounidense, seguido mayoritariamente, ha pretendido dotar de fiabilidad el resultado de los análisis y estudios técnico-científicos que apoyan al derecho, con un solo fin, reforzar el papel de los jueces en la prueba pericial en su admisión y valoración²⁷. Este esfuerzo pretendió homogenizar parámetros de la prueba pericial para su validez en el proceso penal, pensando en la presunción de inocencia; sin embargo, en casos como la determinación de la falsedad de los *Deepfakes*, el espacio de tiempo que debe transcurrir hasta que se superen los criterios *Daubert* es incierto, operando en perjuicio del inculpado. De aquí el calificativo de “al revés”.

Bajo esta óptica es que, con anterioridad, se aseguró la reciente imposibilidad de oponerse objetivamente a los *Deepfakes* aún durante el juicio oral, estado de impotencia que ha venido para quedarse durante un buen tiempo, con la esperanza puesta en que, más pronto que tarde, se desarrollen técnicas probadas suficientemente frente a errores, revisiones y publicaciones por otros científicos, la indicación de acierto de la técnica utilizada, el mantenimiento de estándares de calidad y el consenso de la comunidad científica sobre la fiabilidad de la técnica a utilizar, de tal forma que sea posible alcanzar resultados periciales

²⁴ BLÁZQUEZ MORENO, R.: “*Deepfakes en el procedimiento probatorio*”, A Coruña, s.l., s.f., pp. 244–247.

²⁵ JIMÉNEZ MONTAÑÉZ, M.A.; VILLALUENGA DE GARCÍA, Susana y VALMAÑA OCHAITA, Alicia (eds.): “*El valor de la persona en tiempos de la inteligencia artificial*”, Valencia, Tirant lo Blanch, s.f., p. 305 (contribución de Jesús Punzón Moraleda)

²⁶ PONCE SOLÉ, J.: “*Inteligencia Artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*”, Revista General de Derecho Administrativo, n.º 50, 2019, pp. 46–47.

²⁷ NIEVA-FENOLL, J.: “*Repensando Daubert: La paradoja de la prueba pericial*”, documento de módulo 1, s.l., s.f.

capaces de hacerlos valer en el proceso penal²⁸. Incluso, tal cual lo reseña Miquel Julià-Pijoan hablando de la prueba neurocientífica, habrá que esperar del mismo modo la interpretación que el derecho podrá realizar respecto a la terminología científica utilizada en este tipo de pericias²⁹ y en donde se señala de falso el contenido digital.

Tristemente, la práctica del peritaje informático y la incorporación de sus resultados al proceso, requieren un lapso extremadamente prolongado. Mientras tanto, los *Deepfakes* podrán seguir haciendo de las suyas en la vulneración de derechos. Así las cosas, la esperanza en esta práctica probatoria parece desalentadora.

6. CONCLUSIONES

Los sistemas de inteligencia artificial generativa, al encontrarse al alcance de toda persona, permiten la posibilidad de producir o crear *Deepfakes* sin medida y da manera descontrolada.

La regulación o esfuerzos normativos no han dado cobertura efectiva en la prevención de los impactos perjudiciales de los *Deepfakes* en los procesos judiciales; por lo que, deben tomarse acciones concretas.

Se propone el *Compliance Digital*, pensado en la implementación de protocolos preventivos en el manejo de la evidencia digital (debidamente diligencia), exigido al Ministerio Público Fiscal, Policía, Jueces y Tribunales, con el objetivo principal de evitar el pronunciamiento de decisiones amparadas en *Deepfakes* y que restrinjan derechos y garantías fundamentales, al mismo tiempo, sirva al operador administrativo o judicial como excluyente o atenuante al momento de deducir responsabilidades. Este protocolo podría incluir: a) la creación de una unidad técnica especializada en evidencia digital, adscrita al ente encargado del cumplimiento; b) el llenado de formularios por la persona que ofrece la evidencia digital, que incluya una precisa lectura de las consecuencias de su falsedad y la aceptación de responsabilidades; y c) separar la evidencia aportada por particulares de la obtenida al azar en investigaciones, recomendando que, en ambos casos, deberá pasarse un filtro técnico-científico de exclusión por falsedad.

La ampliación del delito de Fraude Procesal y delitos falsarios, incorporando el uso de *Deepfakes* en los procesos judiciales o en las diligencias previas a su iniciación, podría contribuir a evitar este tipo de prácticas maliciosas, acompañado que sea de una buena política criminal de difusión, explicando a la población en general las consecuencias penales y administrativas de este tipo de conductas y exhibiendo la voluntad del Estado en investigarlo y sancionarlo.

²⁸ *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993); *General Electric Co. v. Joiner*, 522 U.S. 136 (1997); *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999).

²⁹ JULIÀ-PIJUAN, M.: “La relación del sistema penal y la neurociencia desde los conceptos, los significados y las estructuras”, s.l., s.f.

La prueba pericial de extracción y análisis de información, en su momento, será la idónea para la averiguación de la falsedad de la evidencia digital, particularmente si se establece dentro de sus puntos de pericia la determinación de *Deepfakes*. Obviamente, su nivel de validez y aceptación dependerá del esfuerzo técnico-científico que permita alcanzar y/o superar los criterios *Daubert*.

El tiempo que tarda la entrega de resultados de la extracción y análisis de la información como prueba pericial, en la actualidad, no parece adecuarse a la necesidad de descubrir oportunamente la existencia de *Deepfakes* en los procesos judiciales o en la investigación previa; no obstante, la ruta de probatoria de averiguación es, y seguirá siendo, por medio de ésta. En tal sentido, tal cual acontece en el tratamiento de investigaciones relacionadas con delitos sexuales y algunos delitos económicos, previo a decidir sobre la restricción o limitación de derechos y garantías fundamentales, debe requerirse la práctica de informes preliminares o peritajes informáticos, con los que pueda excluirse o reducir la posibilidad de evidencias falsas.

BIBLIOGRAFÍA

“La prueba pericial. Consideraciones sobre la prueba pericial y su valoración en la decisión judicial”, REDEA – Derechos en Acción, año 2, n.º 4, Invierno 2017, p. 131, disponible en: <https://www.corteidh.or.cr/tablas/r37709.pdf>.

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR: *Ley de fomento a la inteligencia artificial y tecnologías*, 2024, disponible en: <https://www.asamblea.gob.sv/leyes-y-decretos/view/6137>.

BLÁZQUEZ MORENO, R.: “*Deepfakes en el procedimiento probatorio*”, A Coruña, s.l., s.f., p. 226.

BLÁZQUEZ MORENO, R.: “*Deepfakes en el procedimiento probatorio*”, A Coruña, s.l., s.f., pp. 244–247.

CENTRO DE INVESTIGACIONES SOCIOLÓGICAS (CIS): *Barómetro de marzo 2024. Avance de resultados*, 2024, disponible en: https://www.cis.es/documents/d/cis/es3486marMT_a.

COLOMA CORREA, R; PINO YANCOVIC, M; MONTECINOS SANHUEZA, C. “*Fundamentación de sentencias judiciales y atribución de calidad epistémica a las declaraciones de testigos en materia procesal penal*”. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, n.º XXXIII, Valparaíso, segundo semestre de 2009, pp. 303-344.

COMISIÓN EUROPEA: *Eurobarómetro especial 518 – Actitudes hacia el impacto de la inteligencia artificial y la robótica*, 2023, disponible en: <https://europa.eu/eurobarometer/surveys/detail/2959>.

CORTE INTERAMERICANA DE DERECHOS HUMANOS: *Opinión Consultiva OC-24/17: Medio ambiente y derechos humanos*, 7 febrero 2018, disponible en: <https://www.corteidh.or.cr/tablas/r30570.pdf>.

DATASCIENSTEST: *Todo sobre John McCarthy*, s.f., disponible en: <https://datascientest.com/es/todo-sobre-john-mccarthy>.

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993); *General Electric Co. v. Joiner*, 522 U.S. 136 (1997); *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999).

HIGH COURT OF JUSTICE (UK): *Ayinde v. London Borough of Haringey and Al-Haroun v. Qatar National Bank*, 5 junio 2025, disponible en: <https://www.judiciary.uk/wp-content/uploads/2025/06/Ayinde-v-London-Borough-of-Haringey-and-Al-Haroun-v-Qatar-National-Bank.pdf>.

HIGH COURT OF JUSTICE (UK): *Olsen v. Finansiell Stabilitet AS*, 16 enero 2025, disponible en: <https://www.judiciary.uk/wp-content/uploads/2025/01/Approved-Judgment-Olsen-v.-Finansiell-Stabilitet-AS.pdf>.

INFOBAE: “*ChatGPT tuvo mayor popularidad con el anuncio de nuevos lanzamientos y ya cuenta con 400 millones de usuarios*”, 7 marzo 2025, disponible en: <https://bit.ly/3ZUdQc4>.

JIMÉNEZ MONTAÑÉZ, M.Á./VILLALUENGA DE GARCÍA, S./VALMAÑA OCHAITA, A. (eds.): “*El valor de la persona en tiempos de la inteligencia artificial*”, Valencia, Tirant lo Blanch, s.f., p. 305 (contribución de J. Punzón Moraleda), disponible en: <https://biblioteca.nubedelectura.com/cloudLibrary/ebook/show/9788410954755>.

JULIÀ-PIJUAN, M.: “*La relación del sistema penal y la neurociencia desde los conceptos, los significados y las estructuras*”, s.l., s.f.

NIEVA FENOLL, J.: “*Teoría General del Proceso (Derecho Procesal I)*”, Valencia, Tirant lo Blanch, s.f.

NIEVA-FENOLL, J.: “*La razón de ser de la presunción de inocencia*”. InDret Revista para el Análisis del Derecho, 1-23.

NIEVA-FENOLL, J.: “*Repensando Daubert: La paradoja de la prueba pericial*”, documento de módulo 1, s.l., s.f.

OTERO, J. M.: “*El derecho siempre va detrás de la sociedad, debe adaptarse a la realidad en que se vive*”, La Opinión A Coruña, 17 noviembre 2019, disponible en: <http://bit.ly/4kgzVZI>.

PARLAMENTO EUROPEO: *¿Qué es la inteligencia artificial y cómo se usa?*, 27 agosto 2020, disponible en: <https://bit.ly/44y78tY>.

PONCE SOLÉ, J.: “*Inteligencia Artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*”, *Revista General de Derecho Administrativo*, n.º 50, 2019, pp. 46–47.

PUERTA LUIS, L.-R.: “*La prueba en el proceso penal*”, s.l., s.f.

RUSSELL, S./NORVIG, P.: “*Artificial Intelligence: A Modern Approach*”, 4.ª ed., Upper Saddle River, NJ, Pearson, 2021, disponible en: <https://bit.ly/4exLGKa>.

RUVALCABA GÓMEZ, C./PADILLA PADILLA, R.: “*Repensando los Derechos Humanos en tiempos de Inteligencia Artificial*”, en: *Inteligencia Artificial y Derechos Humanos: debate actual y de futuro*, Tomo V, Valencia, Tirant lo Blanch, s.f., p. 178.

SALAZAR C., A.: “*La inteligencia artificial vs la inteligencia humana*”, *Duazary*, vol. 15, n.º 3, 2018, pp. 249–250, disponible en: <https://bit.ly/46kwrC1>.

SAVIGNY, F. C.: “*Los fundamentos de la ciencia jurídica*”, Santiago de Chile, Ediciones Olejnik, 2019.

UNIÓN EUROPEA: *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)*, *Diario Oficial de la Unión Europea*, 2024, disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689>.

UNIVERSIDAD INTERNACIONAL DE VALENCIA: “*Inteligencia artificial, ventajas y desventajas*”, 5 marzo 2024, disponible en: <https://n9.cl/8obch>.