Escuela de Derecho
Tipo de documento: Tesis de maestría

Maestría en Derecho Penal

La utilización de Inteligencia de Fuentes Abiertas en la Investigación Penal y los problemas que implica su admisibilidad a la luz de la IA

Autoría: Colasurdo, Matías Ariel
Año: 2025

UNIVERSIDAD TORCUATO DI TELLA

ESCUELA DE DERECHO

MAESTRÍA EN DERECHO PENAL

Tema de tesis: La utilización de Inteligencia de Fuentes Abiertas en la Investigación Penal y los problemas que implica su admisibilidad a la luz de la IA.

Matías Ariel Colasurdo

Legajo: 21R2712

DNI: 41.028.803

Tutora: **Diana Veleda**

Lugar y fecha: Buenos Aires, 13 de octubre de 2025.

Firma tutor

RESUMEN

Este trabajo tiene por objeto examinar los problemas epistémicos y normativos de las pruebas de fuentes abiertas, también conocidas como OSINT, es decir, analizar si son seguras para los objetivos de averiguación de la verdad y respecto de algunos principios normativos propios del proceso penal. Todo esto será analizado a la luz del auge de la Inteligencia Artificial en nuestra sociedad, y de la problemática que puede presentarse a partir de ella con las pruebas de fuentes abiertas, y a partir de ello se ofrecerán criterios concretos y recomendaciones para el mejor tratamiento de este tipo de pruebas.

PALABRAS CLAVE: OSINT – Confiabilidad probatoria – Inteligencia artificial – Fuentes abiertas – Procesal penal.

ABSTRACT

This work aims to examine the epistemic and normative issues of *open-source intelligence* (OSINT) evidence. Specifically, it seeks to analyze whether such evidence is reliable for truth-seeking purposes and compatible with the normative principles inherent to criminal proceedings. This analysis will be conducted in light of the rise of Artificial Intelligence in our society. Once the challenges associated with open-source intelligence are identified, criteria or recommendations will be proposed to ensure the proper handling of this type of evidence.

KEYWORDS: OSINT – Evidentiary Reliability – Artificial Intelligence – Open Sources – Criminal Procedure.

ÍNDICE:

Universidad Torcuato Di Tella – Maestría en Derecho Penal
Matías Ariel COLASURDO*
colasurdomatias@gmail.com

1 Introducción:

La Inteligencia de Fuentes Abiertas (OSINT) podría ser definida como la "inteligencia recopilada de fuentes disponibles públicamente y que no requieren métodos de recuperación encubiertos o clandestinos" (Sampson, 2017, p. 1). Ejemplos de fuentes abiertas serían las redes sociales como *Facebook, Instagram, YouTube*. Otro tipo de fuentes abiertas son las entrevistas, artículos periodísticos, entre otros, es decir, toda información disponible públicamente. Este tipo de información introducido al proceso penal reviste una gran importancia para llevar adelante una instrucción exitosa de las causas penales por parte de los Agentes Fiscales de las distintas dependencias. En definitiva, la evidencia OSINT es de gran ayuda en los procesos penales dentro de una sociedad influida de gran manera por las TICs (Tecnologías de la información y comunicación).

La OSINT es una herramienta que este último tiempo ha logrado obtener una mayor resonancia en nuestra sociedad. Entre otras razones, esta mayor resonancia fue impulsada por el conflicto bélico entre Rusia y Ucrania, donde por ejemplo gracias al "Crowdsourcing" o "Colaboración colectiva" diversas organizaciones fueron recolectando evidencia a través de internet para luego ser presentada ante la Corte Penal Internacional (CPI) a los fines de lograr obtener una rendición de cuentas por parte de los autores[1].

El problema que presenta OSINT en el siglo XXI se debe al auge de la "Inteligencia Artificial" -en adelante IA- pues a través de ella se podría, por ejemplo, llegar a atribuir autoría de un hecho criminal a aquel que nada tuvo que ver con el delito en cuestión, más adelante serán presentados ciertos ejemplos en los cuales se pondrá en

* Universidad de Belgrano. Universidad Torcuato Di Tella. Este trabajo está dedicado a mi Familia por su apoyo constante a lo largo de este camino. A mi tutora, Diana Veleda, por su gran dedicación y enseñanza, que ayudaron a hacer posible este trabajo.

[1] Podemos mencionar como referencia la labor llevada a cabo por el Cuerpo de Verificación Digital de Amnistía Internacional, que comprende "una red de más de 100 estudiantes de múltiples disciplinas de seis universidades asociadas que autentican vídeos e imágenes encontradas en redes sociales para apoyar la investigación en derechos humanos"https://www.amnesty.org/es/latest/press-release/2019/12/amnesty-international-updates-citizen evidence-lab-for-cutting-edge-open-source-human-rights-investigations/ publicado el 11/12/19, recuperado el 25/03/25.

evidencia como ello podría ocurrir. A modo de adelanto debemos de saber que se debe a lo que se conoce como "*Deepfake*", este término se refiere a una imagen, audio o también un video que presentan una falsedad en su contenido, pero que aparentan ser reales a través de una gran calidad en su falsificación muchas veces gracias a la utilización de la Inteligencia Artificial.

Este trabajo tiene como objeto analizar la prueba OSINT, en un contexto de auge de la IA, a la luz de ciertas preocupaciones epistémicas en torno a su confiabilidad, con respecto al objetivo de averiguación de la verdad o correcta determinación de los hechos como objetivo de la actividad probatoria. Y también de preocupaciones normativas, ya que la utilización de OSINT podría traer aparejada la violación de ciertas garantías constitucionales dentro del proceso penal.

Concretamente, con respecto a las preocupaciones epistémicas, sostendré que la evidencia OSINT debiera recibir un tratamiento diferenciado con respecto a otro tipo de pruebas, ya que es posible fundamentar una suerte de *presunción de falta de autenticidad* (o de baja confiabilidad). Sobre ese tratamiento diferenciado, propondré algunas medidas concretas, ya sea como algunos cuidados en la cadena de custodia del material, como la realización de un peritaje previo obligatorio, y también otras medidas más generales, relacionadas con la capacitación de los operadores del sistema.

Con relación a las preocupaciones normativas, analizaré aquellas relacionadas con la falta de previsión normativa de estas pruebas y, en conexión con ello, con la posible injerencia en ámbitos íntimos. Al respecto, sostendré que si bien es deseable la regulación de esta clase de evidencias, no sería necesaria una autorización legal o judicial específica en aquellos casos en los que involucren injerencias *nimias* en la intimidad, algo que, como también sostendré, es posible en el ámbito digital, cuando son los propios usuarios quienes "descorren el velo de protección" de dichos ámbitos.

De esta manera, el trabajo aborda un asunto novedoso, porque el Ministerio Publico Fiscal, como así también los juzgados y tribunales de nuestro país, se encuentran hoy en un escenario que hasta hace pocos años era impensado, ya que la inteligencia artificial no era un tema hablado con frecuencia y las normas no suelen avanzar a la misma velocidad que lo hace la tecnología. Así, el presente trabajo contribuirá a brindar al lector una noción de gran relevancia con respecto a la evidencia OSINT y los problemas que se volverán cada vez más comunes en los próximos años en nuestro país

a raíz del auge de la IA, y también ayudará al personal de la administración de Justicia a prestar mayor atención a las evidencias presentadas en las causas que los ocupan.

2 ¿Qué es OSINT? Dos casos problemáticos específicos: Inteligencia Artificial y *Deepfake*.

La forma en que se lleva a cabo la instrucción de las causas penales fue evolucionando a la par del avance tecnológico y, con este avance, nacieron nuevas herramientas que ayudan al fin de la actividad probatoria del proceso penal, entendido este como la "averiguación de la verdad"[2], y que por lo tanto también ayudan a la labor de los Agentes Fiscales. También evolucionó la manera en que se cometen los crímenes, las estafas ahora pueden ocurrir en línea, los delitos que atentan contra la integridad sexual de los menores también pueden cometerse en la red, entre otros actos criminales que pasaron al plano de la virtualidad.

Con este avance tecnológico que hubo en la sociedad aparecieron las fuentes abiertas de información, por ejemplo, las redes sociales, que son muchas veces una excelente herramienta para obtener evidencia, ya sea porque, por ejemplo, el imputado o la victima compartió una fotografía, una geolocalización, o incluso una conversación de "chat" que termina siendo un elemento probatorio de valor para la causa. Estos elementos, que comparten con conocidos o al público en general, pueden servir como evidencia en las investigaciones penales. De esta manera nació un nuevo y moderno método de investigación que puede ser una gran herramienta, pero también una herramienta problemática.

Como bien mencionamos en la Introducción, OSINT significa *Open Source Inteligence* — "Inteligencia de fuentes abiertas" —, y la podemos definir como un método de investigación donde se recurre a las fuentes disponibles públicamente. Según Nihad A. Hassan y Rami Hijazi (2018), en el caso de internet tenemos foros, blogs, redes sociales, registros Whois, web oscura, direcciones IP, pero también constituyen fuentes OSINT los medios de comunicación, la televisión, diarios, también libros, revistas e

[2] Ferrer Beltrán (2022), pp. 16-17. El autor explica que el razonamiento probatorio "parte de la asunción de los postulados de la denominada concepción racionalista de la prueba. Dicha concepción tiene como punto central […] la asunción de la averiguación de la verdad —como correspondencia con el mundo— como objetivo institucional de la prueba en cualquier tipo de proceso judicial".

incluso fotos y videos los cuales contienen metadatos[3], y finalmente tenemos la información Geoespacial, como por ejemplo los mapas (Hassan & Hijazi, 2018, p. 5).

Con respecto a este método "sus aplicaciones abarcan una amplia gama de casos de uso, desde el crimen organizado, la lucha contra el terrorismo […] hasta la detección de fraudes y la lucha contra el lavado de dinero" (Fivecast, s.f., p. 3). Además, las investigaciones OSINT cuentan con la ventaja de estar al alcance de todos, desde la Policía, Ministerio Público, Poder Judicial, hasta personas ajenas a la Administración de Justicia.

La Oficina de las Naciones Unidas contra la Droga y el Delito clasifica las investigaciones penales en que se utilice OSINT en ciertas etapas. La primera es la identificación de información útil en función de un objetivo, en segundo lugar, la validación de esos datos obtenidos, en tercer lugar se los analiza para certificar que sea lo que pretende ser y finalmente tendremos la producción, donde se incorpora la información recabada en un dispositivo de almacenamiento para que pueda ser presentado ante el organismo de Justicia. (UNODC, s.f.).

Este tipo de investigaciones son de gran ayuda debido a que se puede obtener información de un gran valor para la instrucción y posterior juicio de una causa penal, por ejemplo: horarios, días y lugares en que ocurrió un hecho delictivo, y por supuesto, sus partícipes.

En resumidas cuentas, el uso de OSINT hace que exista mayor celeridad en la instrucción de las causas penales volviéndolas más eficientes, dotando a los Jueces que intervienen en la etapa de Instrucción como también a los Jueces de Juicio de mayores recursos para fundar sus resoluciones, condenas y/o absoluciones.

Las investigaciones OSINT se pueden hacer manualmente, como también de manera automatizada. En el primer caso, sin utilizar software alguno para la búsqueda de evidencia, se realiza manualmente por parte de los agentes estatales a través de, por ejemplo, buscadores de internet. En el segundo caso, implica la implementación de Software dedicados a búsquedas OSINT. Entre otros sistemas, podemos mencionar como ejemplo el "Software Clearview AI"[4]. Los sistemas automatizados OSINT están

[3] Los metadatos son los "datos" de los datos, en ellos se puede encontrar el creador del documento, como también día, mes y horario de creación.
[4] Forbes Argentina. *Multa de 30 millones: el escándalo detrás de la base de datos ilegal de rostros.* Recuperado

"basados en la información pública de las redes sociales y donde hay una forma de filtrado"[5].

2.1 El problema de la Inteligencia Artificial:

No hay consenso en lo que hace a la definición de la Inteligencia Artificial (IA), la Comisión Mundial de Ética del Conocimiento Científico y la Tecnología nos dice que a esta se la debe de entender como "máquinas que imitan ciertas funcionalidades de la inteligencia humana, como la percepción, el aprendizaje, el razonamiento, la resolución de problemas, la interacción lingüística e incluso la producción de trabajos creativos" (UNESCO, 2019). Otra de las definiciones es la dada por el Grupo de expertos de alto nivel sobre Inteligencia Artificial de la Unión Europea (2018), que la define como un "sistema de software […] y hardware diseñado por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital, percibiendo su entorno, a través de la adquisición e interpretación de datos, razonando sobre el conocimiento, procesando la información y decidiendo las mejores acciones para lograr el objetivo dado" (Gobierno de España, 2023, párr. 1).

En síntesis, lo central en cuanto a estas definiciones que tenemos que tener en cuenta a los fines de este trabajo es la capacidad de la IA de razonar imitando la inteligencia humana y de utilizar esa capacidad para cumplir un objetivo a través de la implementación de su creatividad. Esta capacidad de generar "creaciones" se conoce como IA generativa, y es este tipo de IA el mayor problema para las investigaciones OSINT, ya que es capaz de producir distintos tipos de materiales, ya sea creando texto, imágenes, audios, e inclusive música. Este tipo de IA se utiliza para, por ejemplo, "crear "arte" que luego se subasta por grandes sumas de dinero e inclusive temas musicales que imitan a compositores reconocidos" (Velarde, 2019, p. 43). La IA generativa "está

el (20/05/2025) https://www.forbesargentina.com/innovacion/multa-30-millones-escandalo-detras-base-datos-ilegal-rostros-n58909. Este motor de búsqueda de rostros mediante IA permite buscar en segundos con solo una captura de la cara del sospechoso, entre 60 mil millones de imágenes fáciles, brindando la información disponible en las Fuentes Abiertas relativas a la persona, nombre, dirección, profesión, etc. No importa si esa información fue borrada o es privada, si en algún momento fue pública, el sistema la almacena. Clearview fue sancionada y censurada en múltiples ocasiones por infringir las estrictas normas de protección de datos GDPR de la Unión Europea, incluidas varias multas de organismos de control de Italia, Grecia y Francia y sentencias que consideran ilegal la tecnología de empresas similares de Alemania y Austria. En Argentina no existe una regulación, al menos actualmente, que establezca que aplicación OSINT debe de utilizarse y de qué modo, las fuerzas de seguridad y personal del MPF utilizan distintos Softwares de manera "libre", desconociéndose la "confiabilidad" del resultado que proporcionan esas herramientas.

[5] Trottier Daniel. (2012) *Coming to terms with social media monitoring: uptake and early assessment*, Sage, P. 326. Por Ejemplo, interceptar todos los tweets que se originan […] y evaluarlos seleccionando aquellos tweets que contienen una amenaza de bomba y calificar esa amenaza de bomba de acuerdo con su credibilidad y el riesgo real que representa.

basada en redes neuronales avanzadas con la capacidad de producir texto sintético, imágenes, video y audio altamente realista […] se caracteriza por una mayor accesibilidad, sofisticación y capacidad de persuasión. Con estas características, la IA generativa ahora puede ayudar a crear y difundir información falsa, aparentemente creíble de forma rápida y sin esfuerzo" (Chu-ke & Dong, 2024), este tipo de IA es, en gran medida, culpable por la desinformación que existe en Internet, tal es así que entre el "1 de enero de 2022 y el 1 de mayo de 2023, el número relativo de artículos de noticias sintéticas aumentó un 57,3% en sitios web convencionales y un 474% en los sitios de desinformación" (Hanley & Durumeric, 2024, p. 1). En muchos de estos casos se utiliza IA generativa para crear *Deepfake*. "La tecnología detrás del *Deepfake* consiste en algoritmos de aprendizaje complejos llamados *Deep learning* y redes generativas antagónicas (*GANs*). Estos sistemas ven la inmensidad de datos visuales y de audio para aprender patrones y reproducirlos de manera fiel en nuevas producciones" (Molina, 2025, p. 206).

Esta desinformación que produce el *Deepfake* y que se puede encontrar en las redes abiertas de información puede ser captado por las herramientas OSINT y luego utilizado en los procesos penales como prueba contra el imputado o incluso en favor del imputado, generando un engaño en el personal judicial y obteniendo así una resolución injusta.

2.2 Deepfake:

El mayor problema para las Investigaciones que utilicen OSINT es el denominado "*Deepfake*".[6] Este tipo de material fue creciendo exponencialmente con el auge de la IA, las redes sociales se inundaron de este. En la justicia argentina aún no es tenido muy presente de qué trata, debido probablemente a la falta de capacitación del personal del Poder Judicial.

¿De qué estamos hablando cuando nos referimos a *Deepfake*? Para Moyano se trata de "una simulación de sonido, imagen o vídeo que induce al receptor a pensar que es verdad […] consiste en la aplicación de una serie de algoritmos de aprendizaje para

[6] El pasado 19 de mayo de 2025 se sanciono en los Estados Unidos la ley federal *take it down* consistente en penalizar la creación y difusión de contenido intimo no consensuado, tanto sea mediante IA o no, obliga a las plataformas digitales, sin ser necesario una orden judicial, a eliminar imágenes íntimas no consentidas sean o no con Inteligencia Artificial. Es decir, contenido *Deepfake*, esto debe ocurrir en un máximo de 48hs desde la notificación a la plataforma, la norma prevé penas de hasta 3 años de prisión y establece responsabilidad directa para los sitios que no actúen con celeridad, puede formular la denuncia la victima o su representante legal.

modificar y crear contenido multimedia. Consiste en manipular un video para que el rostro -e incluso la voz- de una persona sean reemplazados por la de otra, aparentando autenticidad" (Moyano, s.f., párr. 1).

El *Deepfake* no necesariamente tiene que implicar el uso de la IA, es posible adulterar cierto tipo de contenido de otras maneras. Por ejemplo, en el caso de las imágenes, a través de aplicaciones como Photoshop, para hacer por ejemplo "*Face Swap*", método que consistente en reemplazar el rostro de una persona. Por cierto, han surgido diferentes aplicaciones dedicadas específicamente a dicha tarea, pero con el auge de la IA generativa la elaboración de dicho material es mucho más refinada y convincente, lo que conlleva que la posibilidad de advertir la falsedad de dicha imagen sea una tarea más dificultosa, se puede elaborar sin IA, con IA, e incluso combinando IA con otros programas para crear un engaño perfecto[7].

Otra técnica es la denominada "*Lip Synsing*", que consiste en manipular, en un video, los labios de una persona y agregarle un audio para que parezca que la persona dice algo que en realidad nunca dijo, esto se vuelve aún más complicado de detectar debido a que la IA es capaz de hacer una copia de nuestra propia voz y alterar las palabras que se dicen.

Asimismo, otra técnica que existe es la denominada "*Puppet*" o "Marioneta" este método "permite al usuario hacer que el individuo objetivo se mueva de maneras que en realidad no se movían, esto puede incluir movimientos faciales o movimientos de todo el cuerpo"[8].

Por último, tenemos el *Deepfake* de "texto", consistente en, por ejemplo, replicar la escritura de otra persona, y el *Deepfake* de "audio" donde es posible imitar la voz y entonación de otro sujeto.

2.2.1 Casos prácticos sobre *Deepfake* y OSINT: su uso en procesos judiciales:

En este apartado veremos que implicancias prácticas puede tener la utilización de prueba OSINT con material *Deepfake* en los procesos judiciales. Para ello, presentaré

[7] Ejemplo de esto fue la recreación del actor Paul Walker tras su muerte mientras rodaba su película "rápidos y Furiosos 7" los cineastas utilizaron IA combinado con CGI (imágenes generadas por computadoras) para colocar la cara del actor fallecido, imitar sus movimientos, y expresiones, en su hermano, que lo reemplazo en el rodaje de la película.

[8] Homeland Security. (2019). *Increasing Threat of Deepfake Identities,* p. 12. El uso de la IA tiene tanto potencial que incluso la propia marca de lapiceras BIC, en una propaganda lanzada por sus 75 años, utiliza la IA para recrear la letra de Shakespeare en Romeo y Julieta sobre una hoja de papel.

una serie de casos hipotéticos que pueden mostrar la importancia de la problemática para las investigaciones actuales. Asimismo, explicaré en cada caso de qué tipo de problema se trata (p. ej., si es un caso de *deepfake*, si involucra IA, etc.).

Caso 1: "Una persona es acusada de un homicidio en un edificio de su propiedad. La acusación se basa en una serie de pruebas que incluyen huellas dactilares latentes, ADN del cabello, y videos capturados en el vestíbulo del edificio en el que ocurrió el crimen. La persona acusada, se opone a la verificación de su identidad mediante esos videos, basándose en la baja resolución y la falta de claridad en la imagen del rostro. Además, como coartada, presenta ante el tribunal imágenes de video de otro lugar […] que lo coloca irrefutablemente en otro sitio en el momento en que tuvo lugar el crimen" (Homeland Security, 2019, p. 20).

Este caso presenta dos problemas, el de la autenticación de la evidencia biométrica y el de la posibilidad de que el video presentado por la persona imputada constituya un caso de *Deepfake* (que, en particular, sería un caso de *Deepfake puppet*).

Caso 2: Imaginemos que una persona es acusada por el delito de robo agravado, los testigos, que son vecinos del barrio, dicen que vieron al imputado merodeando la zona una hora antes del hecho, y que una hora después lo vieron caminando con los objetos que la víctima declara que fueron sustraídos de su propiedad. Basándose en tales evidencias, el Fiscal pide la aprehensión y luego su detención. Paralelamente, el imputado pide su sobreseimiento y presenta como prueba de que no en el lugar del crimen un certificado médico de un hospital, con la letra exacta de uno de los médicos del hospital donde menciona que ese día fue atendido allí, y en el horario en que ocurrió el crimen.

En este caso, el contenido *Deepfake* sería el certificado médico, el cual fue creado mediante IA logrando imitar la letra del médico del Hospital. Imagínese que, además, el imputado, presenta videos adulterados que lo sitúan en los alrededores de dicho Hospital, esto con el único fin de darle mayor peso a su requerimiento de sobreseimiento. Como puede notarse, un caso así involucraría, *Deepfake* de texto y *Puppet*.

Ahora imaginemos dos casos que se den en el marco de una investigación que implica la utilización de OSINT.

Caso 3: Un sujeto "**A**" que posee problemas de larga data con "**B**" y está empeñado en lograr su detención, crea un perfil falso en una red social con nombre y apellido de "**B**". En este perfil, sube audios, los cuales fueron adulterados mediante IA, que reproducen la voz de "**B**" a la perfección. En estos audios amenaza a "**A**" con matarlo si en el plazo de 48 horas no le entrega una suma determinada de dinero. Asimismo, hay imágenes, también adulteradas, de "**B**" sosteniendo un arma en la mano apuntando a la cámara.

"**A**" hace la denuncia en la comisaría, presenta capturas de pantalla del perfil de la red social de "**B**" donde constan las amenazas hacia "**A**" y la foto del individuo apuntando con el arma. A raíz de esto es que el Fiscal le pide al Juez el allanamiento al domicilio y posterior detención de "**B**" por tales hechos, tal medida se efectiviza, y "**B**" es detenido.

En este caso se trató de evidencia OSINT, disponible el material en una red social, pero que resulto ser contenido *Deepfake*, en este caso se empleó un *Deepfake* de audio y *Face Swap*.

Caso 4: En la Provincia de Salta un niño es secuestrado por una organización criminal, sus captores, para evitar que la Policía logre dar con su paradero, invaden las redes sociales de información falsa, mediante la utilización de cuentas creadas a tal fin, empiezan a llenar las redes de imágenes y videos, adulterados mediante IA, que ubican al menor en otros puntos geográficos de Argentina. La fiscalía, tras encomendar a la Policía tareas investigativas y mediante el empleo de OSINT, se hace eco de la existencia de tales materiales y son agregados en la causa penal como evidencia.

En este caso, el contenido *Deepfake* son las imágenes y videos que fueron subidos a una Red Social, y descubiertos mediante una investigación OSINT, los cuales se armaron para despistar a la Fiscalía y Fuerzas de Seguridad. Las imágenes consisten en el método *Face Swap*.

Ahora bien, la calidad de estas falsificaciones va a depender de los conocimientos de quien los crea, las herramientas que posea, y por supuesto, el poderío económico, en una causa penal, siempre tendrá mayor probabilidad de cometer *Deepfake* aquellos imputados que reúnan estas características, que aquellos que no las posean, y por lo tanto, mayor probabilidad de lograr su impunidad.

Nunca será lo mismo aquel conocedor de informática, que la persona que no posea tal conocimiento, no es lo mismo aquella persona que creció influenciada desde su infancia por las Tecnologías de la Información y la Comunicación (TICS) que aquel que no. Mucho de los servicios de IA que permiten una mayor manipulación de contenido suelen ser servicios pagos, incluso es factible contratar a una persona que sepa de informática y tenga experiencia en la elaboración de este tipo de material para luego ser presentado como prueba en alguna causa judicial.

Como vimos en los cuatro casos anteriores, el *Deepfake* facilitado con el uso de IA generativa puede resultar problemático, y si no se instruye correctamente a los encargados de intervenir en las causas penales ya sean Fiscales, Jueces o Defensores, esto puede traer serios problemas en lo que hace a la averiguación de la verdad y desde ya en la violación de garantías constitucionales tanto del imputado como de la víctima, ya que la evidencia OSINT que se utilice puede estar seriamente contaminada de material falso, dificultando el proceso que lleve adelante la justicia penal.

Tanto los Fiscales y los Jueces deben velar por que la Evidencia que se incorpora a la causa sea verídica, asegurando de esa manera el respeto al debido proceso, el no estar cualificados para averiguar si lo que tienen frente a sus ojos es un contenido *Deepfake*, pone en riesgo tal garantía, por ello es que deben de llevarse a cabo cursos de capacitación obligatoria por parte de las Escuelas de Capacitación tanto del Ministerio Público como del Poder Judicial, abocadas exclusivamente a las Investigaciones OSINT y *Deepfake*, ello a los fines de asegurar que los operadores judiciales encargados de recabar el material probatorio y valorarlo cuenten con una correcta formación a los fines de identificar la evidencia digital OSINT y el *Deepfake* que podría llegar a haber en su contenido, todo ello debido a que “los tribunales son los guardianes (gatekeepers) de la calidad de la prueba que entra en el proceso” (Gascón Abellán, 2021, p. 66), y para desempeñar ese papel adecuadamente es que deben estar constantemente actualizados respecto a la evidencia digital y sus amenazas.

3 Problemas epistémicos de OSINT: la confiabilidad de la prueba.

3.1 Prueba y confiabilidad: riesgos y herramientas de control:

La actividad probatoria en el proceso penal tiene como finalidad la averiguación de la verdad[9]. Para que la prueba logre alcanzar la verdad, o la correcta determinación de los hechos, vamos a necesitar reunir la mayor cantidad de evidencia que sea confiable y relevante para la hipótesis del caso. Por "relevancia" y "confiabilidad" debemos de entender lo siguiente: cuando hablamos de confiabilidad hacemos referencia a cuánto podemos confiar en esa prueba, es decir, cuán segura es como razón para decidir, cuán verosímil es el enunciado probatorio. La confiabilidad se refiere a las razones para "creer que la prueba es verdadera" (Laudan, 2013, p. 177). Sin embargo, el principal filtro epistémico para la incorporación de la prueba es la relevancia, que hace referencia a si la prueba tiene alguna conexión inferencial con la hipótesis del caso (Taruffo, 2008, p. 39; Ferrer Beltrán, 2007, p. 71).

Ahora bien, aclarados estos conceptos, debemos de saber que, si la actividad probatoria en los procesos judiciales está orientada a la correcta determinación de los hechos, entonces debiera tener como finalidad incorporar la mayor cantidad de evidencia relevante posible. Esto es lo que se conoce como "principio de inclusión probatoria", que se basa en un criterio básico de la racionalidad que determina que, cuantas más razones epistémicas he reunido, menor será la chance de error[10]. Si esto es así, es decir, si en principio debemos incorporar toda prueba relevante, entonces no debería importar, al menos en principio, si la misma no es enteramente confiable o cuál es su grado de confiabilidad. Esto es así porque existe un consenso más o menos generalizado en la doctrina en torno a que, como ya dije, la relevancia es el filtro epistémico para la admisión de la prueba y esta se satisface con un requisito "mínimo" —el de la conexión inferencial— y, en principio, no es necesario que el valor probatorio sea "de una determinada medida" o más "robusto" (Veleda, s.f., pp. 9-10). Sin embargo, para Dei Vecchi "la confiabilidad podría tener incidencia en el juicio de relevancia de un modo

[9] Ferrer Beltrán, J. (2007). *La valoración racional de la prueba*, Madrid, Marcial Pons, P.30. Ferrer Beltrán sostiene que la prueba como actividad tendría la función de comprobar la producción de los hechos condicionantes a los que el derecho vincula consecuencias jurídicas o, lo que es lo mismo, determina el valor de verdad de las proposiciones que describen la ocurrencia de esos hechos condicionantes. Y el éxito de la institución probatoria se produce cuando las proposiciones sobre los hechos que se declaran probadas son verdaderas.

[10] Ferrer Beltrán, J. *La valoración racional de la prueba*, P. 42. Beltrán se refiere al principio general de inclusión al decir que es "la admisión de toda prueba que aporte información relevante sobre los hechos que se juzgan. Una prueba es relevante si aporta apoyo o refutación de alguna de las hipótesis fácticas del caso a la luz de los principios generales de la lógica y de la ciencia.

tal que las pruebas muy poco fiables pudieren resultar irrelevantes [...] la carencia absoluta de fiabilidad hará que un elemento de prueba resulte irrelevante. Pues no tendrá idoneidad para alterar en ningún sentido el estatus de justificación epistémica del objeto de prueba" (Dei Vecchi, 2019, p. 37). Entonces, se admitirá toda prueba relevante, sobre todo en la etapa de instrucción, en cambio, en la etapa de juicio —mientras la parte realice el "ofrecimiento probatorio" y guarde vinculación con la hipótesis o teoría del caso de quien la aporta— será admitida. Luego, los jueces valorarán la prueba y le otorgarán un mayor o menor valor probatorio, teniendo en cuenta su confiabilidad y relevancia, todo ello bajo el sistema de la libre valoración de la prueba bajo las reglas de la sana critica[11].

En el caso de la evidencia OSINT, nos encontramos con un tipo de prueba que, a mi modo de ver, merece un tratamiento "diferencial" con respecto al resto de pruebas que pueden encontrarse en el proceso penal. Si bien el resto de las pruebas, en general, no pasan por controles rigurosos de confiabilidad o autenticidad a la hora de decidir sobre su incorporación en el proceso penal, en el caso del elemento probatorio que aquí venimos a tratar, ello resulta de suma importancia. Este es, pues, el primer punto de mi tesis: en los casos de evidencias OSINT, es recomendable incorporar un examen sobre la confiabilidad del elemento —más allá de su relevancia— a la hora de decidir sobre su admisibilidad.

Como dije antes, en general las pruebas no suelen estar sometidas a análisis "anticipados" de confiabilidad. Esta clase de evaluación es propia, en principio, del momento de valoración de la prueba[12]. Sin embargo, propuestas como la que mencioné antes, para el caso de las OSINT, ya han sido ensayadas para otros elementos probatorios que han sido considerados epistémicamente riesgosos.

[11] Gonzalez Lagier, D. (2003). *Hechos y Argumentos (racionalidad epistemológica y prueba de los hechos en el proceso penal*, P. 41. La valoración de la prueba no puede ser una operación libre de todo criterio y cargada de subjetividad, sino que debe estar sometida a "las reglas de la lógica", "las reglas de la sana critica" "de la experiencia" "del criterio racional" […] se pueden dar criterios más precisos que son "las reglas de la sana critica" si se toman algunas de las pautas de racionalidad epistemológica ofrecidos por algunos lógicos y filósofos de la ciencia para justificar las inducciones científicas […] uno de los criterios que los filósofos de la ciencia exigen para que una hipótesis se considere fundamentada es que los datos a partir del cual se infiere la hipótesis sean fiables y precisos.

[12] Veleda, D. (s.f.). *Apuntes sobre la relevancia y la confiabilidad de la prueba*. P. 13. La evaluación anticipada de la medida del valor probatorio de un elemento de juicio puede ser difícil en algunos casos. Como bien sabemos, la valoración de la prueba es una tarea que tiene un componente holístico imprescindible.

Veamos: en el caso de la prueba pericial o de expertos, ha sido sostenido que los magistrados pueden tender a prestar una deferencia exagerada a ese tipo de elemento de juicio; es decir, que puede existir una sobrevaloración del juzgador sobre este tipo de prueba, apoyando demasiado su confianza en lo que manifiesta el perito, sin tener en cuenta la existencia de algún posible riesgo de error, ya sea proveniente del uso de técnicas inválidas o de una comunicación inadecuada de sus resultados por parte del experto[13].

En el caso de la prueba proveniente de fuentes abiertas, existe un problema similar en lo que hace a la valoración judicial. Hay una suerte de "vulnerabilidad epistémica" en donde se tiende a otorgar demasiada confianza a lo que una persona observa en la red, sin preguntarse de antemano si lo que se está visualizando es auténtico o no. Un juez que no esté capacitado en la evolución tecnológica actual puede que pase por alto los riesgos de error que puede traer aparejado el valorar una prueba OSINT sin poner a prueba la confiabilidad, la autenticidad, de ese elemento de juicio.

Para comprender mejor el contenido de la noción de confiabilidad y su aplicación al caso de la prueba OSINT, utilizaré las herramientas conceptuales propuestas por Anderson, Schum y Twining (2015, pp. 99-101). De acuerdo con estos autores, el estudio de la confiabilidad de la prueba se encuentra conformado por tres factores: la autenticidad, la exactitud y la fiabilidad.

Autenticidad: los autores nos dicen que la autenticidad, como elemento más importante para evaluar de la evidencia, corre riesgo cuando la prueba fue ideada para engañar o cuando pasó por muchas manos. Los autores nos dan el siguiente ejemplo, "E* representa la prueba (de algún tipo) sobre el evento E. Del solo hecho de que esta prueba E* diga que el evento E ocurrió no se sigue que E haya ocurrido. De hecho, de E* un decisor solo puede inferir, en algún grado, que el evento E ocurrió" (Anderson, Schum & Twining, 2015, p. 94).

> [P]or ejemplo, la prueba E_2* que consiste en una fotografía, supuestamente muestra el evento E_2, esto es, que Frank estaba en frente del Banco poco

[13] Gascón Abellán, M. (2021). *Ideas para un "control de fiabilidad" de las pruebas forenses. Un punto de partida para seguir discutiendo*. En Manual sobre derechos humanos y prueba en el proceso penal, P. 56. The Innocent Project estima que el uso de ciencia forense mala o defectuosa (incluyendo disciplinas invalidas o no confiables, insuficiente validación de una técnica de análisis, testimonios expertos exagerados, imprecisos o equívocos) […] es el segundo factor contribuyente a las condenas erróneas y está presente en el 52% de las exoneraciones conseguidas hasta ahora por el Proyecto mediante técnicas de ADN.

después de que aquel fuera robado el 4 de marzo a las 3 pm. La persona que toma la decisión deberá estar atenta a la autenticidad de esa foto. Esta foto puede haber sido adulterada en varias formas; también pudo haber sido tomada otro día o a otra hora. Los asuntos de credibilidad constituyen fuentes muy importantes de duda, pero hay otras dudas que surgen cuando intentamos relacionar las pruebas a las hipótesis (Anderson, Schum y Twining, 2015, p. 94).

Exactitud: la exigencia de la exactitud tiene que ver con respecto a si la prueba -generalmente obtenida mediante dispositivos sensoriales- posee una calidad tal que permita visualizar los eventos que pretende probar.

Fiabilidad: Los autores utilizan el requisito de fiabilidad de la evidencia en un sentido distinto al que venimos empleando; nos dicen que un proceso confiable es aquel repetible, seguro y digno de confianza[14]

Veamos ahora cómo aplicar estos conceptos al caso de las pruebas OSINT.

A mi modo de ver, la principal herramienta conceptual que nos informa sobre el problema de confiabilidad de las pruebas OSINT es la autenticidad. Así como un documento puede ser falso, una firma apócrifa, las fuentes OSINT nos enfrentan con falsedades o manipulaciones similares, aunque mucho más difíciles de detectar. Además, desde que se inicia la etapa de Instrucción hasta que se dicta sentencia, es un hecho que la prueba pasará por muchas manos, y cualquiera puede alterar el contenido de la prueba OSINT.

En el caso de la noción de "exactitud", esta parece más bien aplicable a los mecanismos y herramientas desarrolladas para el tratamiento de las pruebas OSINT y que empleen tanto el personal de las Fuerzas de Seguridad como de la Justicia.

Por último, es claro que las pruebas OSINT no pueden someterse a estándares de repetibilidad y precisión, porque no son técnicas o mecanismos periciales. Se trata de evidencia "volátil" que corre el riesgo de desaparecer de las fuentes abiertas, y que tiene la posibilidad de haber sido manipulada.

En definitiva, a mi modo de ver, el concepto más útil para analizar los problemas de confiabilidad de las pruebas periciales es el de *autenticidad*. Teniendo en cuenta esto

[14] Vázquez, C. (2016). *Presentación de la traducción al castellano del Informe del PCAST sobre la ciencia forense en los tribunales penales*. P. 296. La validez de los fundamentos de un método científico-forense requiere que se haya demostrado, basándose en estudios empíricos, que es repetible, reproducible y preciso… La validez de los fundamentos, entonces, significa que un método puede, en principio, considerarse fiable.

y lo explicado en el apartado anterior, creo que he podido demostrar que existen múltiples fuentes de engaño y confusión provenientes de las actuales herramientas digitales que permiten la manipulación de este tipo de información, de manera que, a diferencia del caso de cualquier prueba ordinaria, —en la que, como regla, su confiabilidad se presume hasta su contradicción en el debate—, considero que aquí la posición del juzgador debe ser más prudente. Algo así como una "presunción de baja confiabilidad" o, mejor dicho, una "presunción de falta de autenticidad", hasta que se demuestre lo contrario. Además, como veremos más adelante, propondré un arreglo institucional concreto para solucionar este problema: un peritaje de autenticidad previo obligatorio.

En resumen, así como la prueba pericial o de expertos, dada a la exagerada deferencia que tiene el juez sobre esta, puede llevar al error en la toma de decisiones, algo similar ocurre con el caso que nos ocupa. Apoyar la confianza sobre prueba OSINT sin tomar los recaudos necesarios puede conducir, de igual manera, al error y, por consiguiente, acarrear la condena de un inocente o la absolución de un culpable.

Tal y como ocurre con la prueba pericial, en el caso de la evidencia de fuentes abiertas existe una especie de *laissez-faire* por parte de las judicaturas. Así como la *Law Comission* de Inglaterra y Gales, propuso con las pruebas periciales estándares más estrictos de admisibilidad, lo mismo debería proponerse con las pruebas de fuentes abiertas, ya que "podrían impedir que algunas pruebas […] de baja confiabilidad […] pudieran formar convicción de culpabilidad respecto de los acusados" (Duce, 2018, p. 232).

Por lo tanto, a diferencia de otros elementos de juicio, una vez que es incorporado este tipo de elemento probatorio al proceso, nos exige la adopción de ciertas medidas con el fin de evitar la posibilidad de error por parte del juzgador. En lo que sigue, intentaré proponer algunos posibles resguardos o criterios para el examen de confiabilidad que propongo.

Entonces, para evitar la posibilidad de error por parte del juez en la toma de decisiones con prueba proveniente de fuentes abiertas, debe de asegurarse la calidad de la evidencia OSINT "dentro del proceso"[15].

[15] Marina Gascón Abellán se refiere a los controles intra y extra procesales en el caso de la prueba pericial. Ocurre

Previo a introducirnos en ello, es importante puntualizar que, si bien no hace al proceso, una política que debería de llevarse a cabo sería lograr acuerdos de colaboración entre las Fuerzas de Seguridad, el Poder Judicial y el Ministerio Público con las compañías donde se alojan los datos de información.

En tanto el contenido disponible en la red resulta ser "volátil", es decir, puede ser eliminado, esto dificulta las tareas a desarrollar por los expertos a los efectos de evaluar la "confiabilidad" de la prueba OSINT. En tal sentido, una cooperación dada a través de convenios con las grandes compañías podría mitigar tal inconveniente y facilitar los peritajes destinados a verificar la confiabilidad o autenticidad de este tipo de prueba en el proceso penal.

Por ejemplo, las compañías abocadas al mundo de las redes sociales pueden conservar registros, metadatos u otra información de interés que puede servir como prueba en una causa penal, tal como fechas de creación de una cuenta, direcciones IP, dirección de correo que se utilizó para la creación. La celebración de convenios entre organismos que facilite la entrega de datos a la justicia otorgaría no solo confiabilidad, sino también celeridad a la investigación penal en curso. Esta sería una manera de comenzar a trabajar en el resguardo de la calidad de la información incluso antes de evaluar su ingreso a los procesos judiciales.

Veamos ahora sí algunos criterios de control "intra procesales".

3.1.1 Asegurar la calidad de la prueba OSINT "en el proceso":

El "control" sobre la prueba debería de extenderse a lo largo de todo el proceso penal. Lo cierto es que no siempre ocurre, ello al menos que hubiere alguna petición de parte que siembre duda sobre algún elemento de juicio en particular. En el caso de la prueba OSINT, el control de la prueba debería de realizarse de "oficio", en tanto pudo haber sido incorporada al expediente prueba que lleve al juez a tomar decisiones erróneas. Por tal motivo, se vuelve imprescindible realizar un control de fiabilidad de la evidencia OSINT una vez que la prueba es incorporada en el proceso penal.

Este control que propongo asegura que la evidencia OSINT conserve su integridad en cuanto a su contenido, previo a que el juez valore ese elemento de juicio.

---

que, en el caso de la prueba OSINT, no es posible desarrollar controles "en su origen", como podríamos hacerlo, por ejemplo, con el correcto funcionamiento de los laboratorios forenses. Entonces, como no tenemos control acerca del origen o producción de estas pruebas, debemos reforzar todavía más su control intra procesal.

Por tanto, es menester que, previamente al dictado de la sentencia, la prueba OSINT haya sido sometida a distintos mecanismos de verificación suficientes a los fines de comprobar su fiabilidad y, en consecuencia, de evitar todo planteos futuros, como podrían ser planteos de nulidad en etapas recursivas, entre otros.

En síntesis, este control de confiabilidad es de especial relevancia, ya que, durante el largo transcurso de un proceso penal y al haber pasado la evidencia por "varias manos", si la prueba OSINT no fue alterada desde su origen, esta podría haber sido alterada o sustituida en el proceso y, en consecuencia, podría llevar al Juez al "error", lo que afectaría el derecho a un debido proceso y podría resultar en la condena de un inocente o la absolución de un culpable. De esta forma, se vería afectado el fin que tiene la etapa probatoria en el proceso penal.

Ahora bien, ¿con qué métodos contamos en el proceso para asegurar la confiabilidad de la evidencia provenientes de fuentes abiertas? Veamos a continuación algunos de ellos.

- **Cadena de custodia**. Es fundamental que se dé cumplimiento a la existencia de una cadena de custodia, donde consten, como datos más relevantes, la descripción de la muestra, su modo de conservación, y los eslabones en la cadena de custodia.[16]

- **Aplicar códigos hash**. El Código es la "huella digital" de la evidencia y consiste en una serie de números y letras que dan fe que esa prueba no ha sido alterada. Si, al momento de verificar la confiabilidad de la prueba, el código "hash" varía, entonces podríamos concluir que la evidencia fue manipulada. Por ello, es prudente verificar, previo al dictado de una sentencia, que el código hash de la prueba OSINT que se utiliza como fundamento de condena, sea el mismo al que existía al momento de ser incorporada la prueba al proceso.

Ahora bien, aunque se cumplan esas premisas, no son suficientes para dar garantía de la confiabilidad del contenido. Estos recaudos, solamente brindan un poco más seguridad al saber que el material, una vez incorporado al proceso, no fue alterado

[16] El Convenio de Budapest en su artículo 29 establece ciertas reglas a tener en cuenta a la hora de conservar medios digitales, tales como precisar a. La autoridad que solicita la conservación b. El delito objeto de investigación y una breve exposición de los hechos relacionados con el mismo c. los datos informáticos almacenados que deben conservarse y su relación con el delito d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos o el emplazamiento del sistema informático; e. la necesidad de la medida de conservación.

por un tercero. Por lo tanto, sigue existiendo el problema de estar frente a prueba OSINT que pueda llevar a error al juzgador en razón de las manipulaciones que pudieron existir en su producción misma. La evidencia, en su origen, pudo haber sido alterada. Por ejemplo, la prueba de fuente abierta que se pretende utilizar y a la que se le aplican estas garantías de protección en el proceso, puede ser un elemento de juicio que fue alterado desde un primer momento al ser subido a la red, por lo que aplicar lo mencionado no da fe de que estemos frente a prueba de fuentes abiertas confiable y auténtica. Entonces, nuestra primera conclusión es que un examen de confiabilidad en el caso de la prueba OSINT debe incluir resguardos sobre la cadena de custodia, pero no puede limitarse a ese examen.

Es necesario que exista un control de confiabilidad, y que se lleve a cabo una vez que la prueba es incorporada al proceso penal. Este control puede ser garantizado por un examen pericial previo obligatorio bajo las reglas de las pruebas definitivas e irreproducibles, debiendo ser efectuada por expertos en el área de IA[17], que pongan en conocimiento al juez sobre si la prueba incorporada a las actuaciones podría tratarse de un caso de *Deepfake*. Es importante que la conclusión del experto sea aportada a la causa previo al debate oral y, por tanto, antes del dictado de la sentencia. A tal fin, sería recomendable establecer un plazo no perentorio y, una vez recibido por escrito el informe pertinente, se debería realizar, con posterioridad, una audiencia preliminar obligatoria a los fines de que deponga oralmente el experto y emita sus conclusiones respecto a la prueba aportada. Asimismo, se cite a las partes a los fines de dar cumplimiento al principio de bilateralidad para que depongan oralmente ante el Juez con los mismos fines.[18]

Asimismo, otra opción, a fin de corroborar la confiabilidad del medio de prueba y tal como se propone con la prueba pericial, consistiría en "educar" tanto al juez como

[17] Así como por ejemplo en los Departamentos Judiciales de la Provincia de Buenos Aires, como puede ser San Isidro, se cuenta con el cuerpo de asesoría pericial, la cual cuenta con psicólogos a los fines de labrar los informes que piden las judicaturas, ¿por qué no podríamos implementar un área integrada por distintos expertos en tecnología con especial énfasis en IA a los fines de remitir las pruebas y que están pasen a ser peritadas en la generalidad de los casos?

[18] En la Provincia de Buenos Aires la Sala Segunda del Excmo. Tribunal de Casación Penal Provincial en autos "L,A. s/ Recurso de casación" estableció la importancia de la notificación a las partes a las pruebas periciales, bajo sanción de nulidad "lo hace a los efectos de proteger los derechos del imputado de controlar el desarrollo de la prueba o nombrar perito a su costa" así, una audiencia previa obligatoria antes del debate oral para que deponga el perito y los abogados en torno a la prueba OSINT podría constituir un caso de actos definitivos e irreproducibles donde seria de importancia que las partes estén presentes para controlar lo que manifiesta el experto y la prueba que se incorpora. TC0002 LP, P 6031 RSD-635-3 S 11-9-2003, Juez Hortel.

al jurado. Esto se debe a las dificultades que existen en torno a este medio de prueba en la actualidad. Con respecto a la prueba pericial, en este sentido, se ha afirmado que "jueces y jurados carecen de conocimiento sobre muchas cosas, como la ciencia y la tecnología, pero no hay ninguna razón para que no puedan dominar adecuadamente los campos relevantes" (Herdy, 2020, p. 92). Téngase en cuenta aquí que, a diferencia de lo que ocurre con la prueba pericial, que abarca muchos campos de estudio muy diferenciados, en el caso de las pruebas OSINT la materia conocible, aunque compleja, se encuentra más circunscripta, lo que debiera mejorar las posibilidades de capacitación. Más allá de estas capacitaciones regulares generales, otra aproximación a esta propuesta educativa podría ser a través de la implementación, tal como ocurre en los EE.UU., en el momento de la admisión de la prueba, de un "consultor experto" o "*technical advisor*" "que pudiera educar básica y rápidamente al juez sobre las cuestiones más elementales" (Vázquez, 2020, p. 45).

Por lo tanto, es necesario tener en cuenta ciertas particularidades que no se presentan en otros elementos probatorios, a los fines de garantizar autenticidad en este medio de prueba tan especial. Por ello, entre otras herramientas, la "educación" a los magistrados y jurados reviste tanta importancia.

Entonces, la prueba OSINT es una evidencia con la que se debe tener especial cuidado una vez que es incorporada al proceso penal, ya que la confiabilidad de ese tipo de prueba debe de ser puesta en "tela de juicio" debido al fenómeno de los *Deepfakes*.

La incidencia de los *Deepfakes* en la prueba OSINT representa un desafío, ya que, como mencioné anteriormente, puede, con relativa facilidad, inducir a engaño a los operadores judiciales. En este sentido, una vez que se incorpora al proceso penal prueba de esta índole, está debe pasar necesariamente por "controles"; a diferencia de otros elementos probatorios, en caso contrario, se pone en riesgo el fin que la prueba tiene en el proceso penal.

En síntesis, la prueba en el proceso penal se encuentra estrechamente vinculada con una finalidad epistémica, la finalidad de la prueba es arrojar luz sobre los hechos pasados, es decir, buscar la verdad, y para que la prueba OSINT cumpla esa finalidad propuse una serie de herramientas de control, en primer lugar hablamos de la posibilidad de lograr acuerdos de colaboración entre las Fuerzas de Seguridad, el Poder Judicial y el Ministerio Público con las compañías donde se alojan los datos de información. En

segundo lugar, vimos herramientas de control "intra procesales" como la implementación de Códigos "hash" y la importancia de la Cadena de Custodia, luego, en tercer lugar, vimos la posibilidad de implementar peritos en IA que pongan en conocimiento al Juez si la prueba incorporada a las actuaciones podría tratarse de un caso de *Deepfake,* vimos la posibilidad de una audiencia preliminar obligatoria a los fines de que deponga oralmente el experto y emita sus conclusiones sobre la prueba aportada. Asimismo, se cite a las partes con los mismos fines, a fin de dar cumplimiento al principio de bilateralidad. Por último, hablamos de "educar" al juez como también al jurado. Como posibilidad mencionamos la implementación de un "*technical advisor*" que pudiera educar básica y rápidamente sobre las cuestiones más elementales.

4 Problemas normativos de OSINT: la validez de la prueba.

4.1 Los límites al principio de inclusión y los fundamentos no epistémicos de la regla de exclusión probatoria:

Como ya señalé anteriormente, uno de los principios que rigen en materia probatoria es el denominado principio de inclusión, bajo este principio "todo lo que tiene utilidad probatoria puede ser admitido como prueba" (Gascón Abellán, 2020, p. 178), es decir, corresponde en principio incorporar toda prueba relevante. Sin embargo, este principio que ordena la recepción de la prueba lógicamente relevante debe tener en cuenta las excepciones de la ley (Anderson, Schum, Twining, 2015, p. 354).

Entonces, si bien la prueba debe ser aceptada y conocida por el órgano judicial, pueden existir razones válidas para excluirla[19]. En el punto anterior nos referimos a la posibilidad de justificar la exclusión de prueba, o algún tratamiento específico sobre su admisión, sobre la base de razones *epistémicas.* En cambio, en este punto me referiré a la inclusión y exclusión de prueba OSINT por razones *no epistémicas o normativas,* es decir, no relacionadas, en principio, con la correcta determinación de los hechos. Dicho de otro modo, la exclusión de la prueba OSINT podría responder a asuntos extra epistémicos, es decir, cuestiones ajenas a la búsqueda de la verdad.

Ahora bien, es generalmente aceptado que la posibilidad de incorporar una prueba no depende sólo de su relevancia, sino también de la legalidad de los

[19] Vera Sánchez, J. (2021). *El principio de Inclusión de la prueba*, P. 94. Este principio de inclusión "ha sido uno de los rasgos más importantes de la *Anglo American Evidence Scholarship* que ha dominado la discusión probatoria del siglo XX".

procedimientos orientados a incorporarla y producirla, de manera que sería nula toda evidencia que se hubiera obtenido en violencia de dichas reglas o, más aun, avasallando los derechos reconocidos por nuestra Constitución. Esta concepción de la regla de exclusión tuvo su origen jurisprudencialmente en los Estados Unidos y fue avanzando rápidamente hacia el resto del mundo[20].

Como explica Dei Vecchi, en estos casos "la no admisibilidad o la exclusión se basan en consideraciones normativas que tiene que ver con la tutela de valores, consideraciones axiológicas, contrastes con la búsqueda de la verdad, casos donde lo que se excluye son razones epistémicas relevantes por razones no epistémicas y tampoco prudenciales" (Dei Vecchi, 2020, p. 43). En estos casos, la prueba a excluirse puede clasificarse como prueba prohibida, prueba ilegal, prueba ilícita, prueba inconstitucional, prueba nula, prueba irregular, o prueba viciada. (Delgado del Rincón, 2012, p. 1).

En definitiva, me ocuparé aquí de ese cúmulo complejo de razones normativas conjugadas y ponderadas" (Dei Vecchi, 2020, p. 44), que podría entrar en juego al analizar la prueba OSINT.

Conforme lo expuesto, incorporar prueba OSINT en violación de normas constitucionales y/o leyes puede tornar esa prueba en "ilícita", y si de esa evidencia se obtiene otro elemento probatorio, por más que se obedezcan las reglas de "juego" del proceso penal, estaríamos frente a prueba ilícita "derivada" y por lo tanto tampoco debe de ser tenida en cuenta por el órgano judicial.

Ahora bien, como dije hacia el comienzo de este punto, la exclusión de prueba ilícita se funda, en principio, en razones no relacionadas con la correcta determinación de los hechos. Sin embargo, hay autores que asocian la finalidad de la regla de exclusión con objetivos epistémicos, porque asocian prueba ilícita con prueba poco confiable. Por ejemplo, para Nieva Fenoll:

> [C]uando se vulnera un derecho fundamental el agente actuante entra en un espacio de total clandestinidad que le otorga un ilimitado campo de actuación, lo que resulta peligrosísimo. Siendo ello así, la vulneración del derecho constituye un indicio absolutamente razonable de que el agente está intentando crear un relato que tiene la más amplia oportunidad de introducir en la escena, manipulando la realidad, sembrando una prueba falsa en el proceso que todo el mundo va a dar por auténtica. En consecuencia, la vulneración de un derecho

[20] En la República Argentina, el fallo más emblemático con respecto a la exclusión de la prueba ilícita es el caso Charles Hermanos dictado por la Corte Suprema de Justicia de la Nación en el Siglo XIX (CSJN, Fallo: 46:36).

fundamental constituye un indicio evidente de falseamiento policial de la realidad (Alan Limardo, 2021:19).

Sin abrir juicio sobre el acierto o error de este fundamento "epistémico" para la regla de exclusión de la prueba ilícita, me ocuparé aquí de las dimensiones normativas del problema, ya que he dedicado la primera parte de este trabajo a proponer algunos arreglos institucionales que podrían ayudar a disminuir los riesgos asociados a la baja confiabilidad de estas pruebas.

4.2 Problemas normativos de legalidad e intimidad:

Antes de continuar con el desarrollo, es necesario advertir que no podré abordar la totalidad de los problemas normativos que podrían surgir con este tipo de pruebas, porque ello podría depender de circunstancias propias de cada caso que son imposibles de prever. Sin embargo, me ocuparé de un problema general de este tipo de pruebas, que se vincula con su reciente desarrollo e implementación, que es su *falta de previsión normativa* y, con ello, su relación con una posible infracción al principio general de reserva de ley. Al respecto, sostendré que una regulación sería deseable, aunque sería exigible centralmente en aquellos casos en los que las pruebas OSINT involucren injerencias del Estado en ámbitos protegidos constitucionalmente. Es decir, mientras la incorporación de evidencia OSINT involucre una injerencia *nimia o bagatelaria* (Pérez Barbera, 2015, p. 57), podría prescindirse de esa autorización. Ahora bien, para trazar esa distinción, analizare una posible injerencia involucrada en el caso de las pruebas OSINT, que es aquella que podría tener lugar en la esfera de intimidad de las personas. Sostendré que, en un buen grupo de casos, dadas las especiales características de los medios digitales, las expectativas de intimidad son menores y, entonces, podría prescindirse de una autorización normativa específica y de una orden judicial. Esto, en cambio, podría ser exigible en otros casos.

4.2.1 Principio General de Reserva de Ley:

En la República Argentina no hay actualmente una legislación que regule las pruebas provenientes de fuentes abiertas y nos oriente en qué casos se debe de llevar a cabo una investigación OSINT y, lo más importante, de qué manera. Por lo que queda al arbitrio del personal judicial llevarla a cabo y establecer los medios, los cuales suelen ser a través de aplicaciones dependientes de compañías privadas, desconociéndose que ocurre con los datos recabados una vez finalizada la investigación penal.

Ahora bien, para Pérez Barbera, "la reserva de ley obliga a que la medida estatal en cuestión este autorizada en forma previa y taxativa, es decir, a través de una norma ya vigente al momento de tomarse esa medida y que se refiera a ella de manera expresa y clara" (2015, p. 46). Además, la CIDH ha afirmado que es fundamental para el correcto desarrollo del proceso penal el establecimiento de una ley debido a que "en casi todos los sistemas legales internos del continente existe el requisito de que los agentes policiales o el personal de seguridad cuenten con una orden judicial para realizar ciertas acciones que se considera que son especialmente intrusivas"[21].

En consecuencia, el hecho de que no exista una ley que autorice el uso de evidencias digitales ya podría implicar un problema normativo grave. Además, la falta de un marco de regulación legal en la Argentina hace que sea más difícil establecer los límites normativos y éticos en las investigaciones OSINT, por lo que podría ser deseable que, al menos para algunos casos, existieran regulaciones a los fines de mitigar los riesgos que implica una investigación de estas características.

Vale resaltar lo siguiente: es de vital importancia que la ley que exista regule las investigaciones que utilicen aplicaciones automatizadas de búsqueda OSINT mediante IA y, dependiendo de la profundidad de la investigación penal —es decir, el nivel de intrusión sobre la privacidad del sospechado—, se deben requerir criterios más estrictos respecto el procedimiento a seguir, las personas autorizadas a llevarlo a cabo y el tiempo en que pueden inmiscuirse en los datos públicos de la persona sospechada.

Por ejemplo, en el caso Escher vs. Brasil de la CIDH (2009), en el que se había interceptado y monitoreado de manera ilegal conversaciones telefónicas entre los imputados, la Corte dijo que "las condiciones y circunstancias generales conforme a las cuales se autoriza una restricción al ejercicio de un derecho humano determinado deben estar claramente establecidas por ley. La norma que establece la restricción debe ser una ley en el sentido formal y material"[22].

En el caso de la interceptación de llamadas telefónicas se ha dicho que "puede representar una seria interferencia en la vida privada, dicha medida debe estar fundada en la ley, que debe ser precisa e indicar reglas claras y detalladas sobre la materia, tales como las circunstancias en que dicha medida puede ser adoptada; las personas

[21] Causa 10.056, informe 38/96, Comisión Interamericana de Derechos Humanos, apartado 82.
[22] Causa Escher vs. Brasil, Comisión Interamericana de Derechos Humanos, apartado 130.

autorizadas a solicitarla, a ordenarla y a llevarla a cabo; el procedimiento a seguir, entre otros elementos"[23].

Por lo que en aquellos casos en los que hay una "razonable expectativa de privacidad", la medida que permita el avasallamiento del derecho fundamental —ya sea derecho a la intimidad u otro— debe: "ser prescrita por la ley; ser necesaria para la seguridad de todos y guardar relación con las demandas justas de una sociedad democrática; […] ser proporcional y razonable a fin de lograr esos objetivos"[24].

En síntesis, en nuestro país se carece de una ley en sentido formal y material que regule las cuestiones relativas a este elemento de juicio, siendo necesaria para el personal que autorice la medida únicamente en el caso de que exista una injerencia en un ámbito protegido constitucionalmente. Esto puede ocurrir cuando la evidencia digital se relacione con ámbitos sobre los que exista una "expectativa razonable de privacidad" por parte de la persona sospechada. Hasta no existir tal regla, debería procederse a la aplicación analógica de las reglas procesales relacionadas con la invasión de espacios de intimidad, como podrían ser las de las intervenciones telefónicas —centralmente, la exigencia de autorización judicial previa—. Exploraré un poco más la relación de la evidencia digital con la intimidad y el alcance de esa "expectativa de intimidad".

4.2.2 Derecho a la Intimidad:

El derecho a la intimidad[25] es uno de los derechos que puede verse vulnerado con la incorporación de prueba OSINT. A este se lo puede definir como "derecho personalísimo que permite sustraer a la persona de la publicidad o de otras perturbaciones a su vida privada, el cual está limitado por las necesidades sociales y los intereses públicos" (Vaninetti, 2020, p. 23). También se puede decir que "es el derecho a mantener intacto un ámbito de reserva individual y que la persona no vea arrastrados al ámbito público detalles de su vida que no quiere exponer […] en tanto ellos no sean antijuridicos" (Vaninetti, 2020, p. 24).

Ahora bien, hoy en día con el auge de la tecnología y la proliferación de las redes sociales, este derecho pueda verse vulnerado con facilidad y, como vimos antes,

[23] Causa Escher vs. Brasil, Comisión Interamericana de Derechos Humanos, apartado 132.
[24] Causa 10.056, informe 38/96, Comisión Interamericana de Derechos Humanos, apartado 60.
[25] Art. 18 de la CN: "…El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación…"

los usuarios que navegan por internet suben datos que pueden resultar de interés para una investigación penal[26]. Pero así como la correspondencia epistolar es inviolable[27] y haciendo una interpretación "dinámica"[28] de la CN resultaría que por correspondencia epistolar debemos entender también los datos subidos en la red, ya sean fotos, imágenes o videos que comparten los usuarios a través de las fuentes abiertas, por tanto, podríamos argumentar que cuenta con la misma protección constitucional. En este punto, es decir, sobre la posibilidad de extender los espacios de protección de la intimidad a nuevos ámbitos, asumo que existe un acuerdo más o menos generalizado, de manera que no desarrollare mucho más el punto.

Sin embargo, aunque pueda reconocerse la tutela de espacios de intimidad en el ámbito digital, es necesario realizar ciertas distinciones. Como veremos a continuación, existen ciertos datos que son propios de ese ámbito, pero otros que, a mi modo de ver, no pueden considerarse abarcados por una "razonable expectativa de intimidad".

4.2.3 Críticas a la supuesta violación del Derecho a la Intimidad en caso de pruebas OSINT:

Aunque una prueba OSINT se considere abarcada por un espacio de intimidad protegido por la Constitución, esto no significa que esa información sea inaccesible, ya que podría restringirse ese derecho, de conformidad con las leyes aplicables, a los fines de tutelar otros valores, como la persecución de los delitos.

Como bien sabemos, los derechos previstos en la CN no son absolutos, sino que son relativos, es decir, tienen limitaciones[29]. La intimidad de la persona puede verse vulnerado de una manera legitima y esto es siempre "que medie un interés superior en

[26] Chaia, R. (2025). *La Prueba Digital,* pág. 32. Mark Zuckerberg, CEO de Facebook, ha dicho que "la edad de la privacidad se ha terminado, que es algo del pasado, que se trata de un derecho que ha muerto en la sociedad moderna.

[27] Dessy Gustavo Gaston s/ habeas corpus, voto de los Dres. Carlos S. Fayt, Enrique Santiago Petracchi y Antonio Boggiano. "La intromisión en la correspondencia epistolar traduce una de las fracturas más graves del ámbito de libertad y privacidad de los hombres. La carta es vehículo del pensamiento y el pensante su exclusivo señor. Sólo él puede disponer la exteriorización de su pensamiento y sólo él puede escoger al destinatario".

[28] La Corte ha propuesto ir más allá de (una mayoría de) criterios que llevarían a "mirar hacia atrás", en busca de los orígenes de la norma para proponer una interpretación "dinámica" que "actualice" el sentido de la Constitución, adecuándola "a la realidad vigente" de la época (i.e CSJN "Chocobar" fallos: 310: 3267).

[29] "…la Constitución no consagra derechos absolutos, y que los consagrados en ella deben ser ejercidos conforme a las leyes que los reglamentan…" (Fallos, t. 305, p. 831 y sus citas; M.116.XXII, 18 octubre de 1988, "Marítima Key Kar, S. R. L. c. Municipalidad de la Ciudad de Buenos Aires s/revocatoria" -Rev. La Ley, t. 1989-A, p. 545, fallo 87.232-; R.335.XX. "Repetto, Inés M. c. Provincia de Buenos Aires s/inconstitucionalidad de normas legales, Verbitsky, Horacio y otros s/apología del crimen.

resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres, o la persecución del crimen"[30].

En una causa penal donde exista un choque de derechos entre la intimidad y la seguridad pública, podría prevalecer, según el caso, el derecho de mayor valor, y en este caso será la seguridad pública, de esta manera "las restricciones deben estar justificadas por objetivos colectivos de tanta importancia que claramente pesen más que la necesidad social de garantizar el pleno ejercicio de los derechos garantizados por la Convención…"[31].

Por supuesto que, de contemplarse que la medida va a comprometer un derecho constitucional, debe existir una evaluación de su proporcionalidad. Tal como ocurre, por ejemplo, previo a resolver un allanamiento donde debe de tenerse en consideración la proporcionalidad de la medida; en el caso de la investigación OSINT ocurre lo mismo. Es importante que el Juez tenga en consideración el "principio de proporcionalidad"; mientras la medida cumpla tal principio, la obtención de elementos de juicio OSINT no debería ser puesta en tela de juicio[32].

Ahora bien, como adelanté, podrían existir casos de evidencia OSINT que no involucren auténticas injerencias en ámbitos de intimidad. Para analizar estos casos, me valdré primero de la noción de "expectativa razonable de intimidad". Aunque esta noción no ha sido específicamente desarrollada por nuestra Corte Suprema, no encuentro razones que la hagan incompatible con su jurisprudencia que, además, en muchos casos hizo uso de los pronunciamientos de la SCOTUS. Por último, en cualquier caso, es una herramienta útil para la interpretación del alcance de la garantía contenida en nuestra Constitución.

El precedente *Katz v. United States* (1967) de la Suprema Corte de Justicia de los Estados Unidos es una decisión fundacional acerca de la noción de "expectativa razonable de privacidad". Allí se estableció que: "la persona cuyos derechos bajo la Cuarta Enmienda supuestamente han sido violados debe haber tenido una expectativa subjetiva de privacidad", y que "esa expectativa debe ser una que la sociedad pueda

[30] Véase. p. ej "Indalia Ponzetti De Balbin c/ Editorial Atlantida S.A. s/ Daños y Perjuicios".
[31] Informe 38/96 de la CIDH, párrafo 58.
[32] Camenzind v. Suiza (1997) "los Estados parte pueden considerar necesario recurrir a medidas tales como las visitas domiciliarias y decomisos para conseguir la prueba material de ciertas infracciones. El TEDH controla la pertinencia y suficiencia de los motivos invocados para justificar aquéllas, así como el respeto del […] principio de proporcionalidad"

reconocer como razonable. Se considera que se han violado los derechos de una persona amparados por la Cuarta Enmienda si se cumplen ambas condiciones", así como que, "de no cumplirse ninguna de ellas, se determinaría que no se violaron los derechos a la privacidad" (Xander de los Reyes, 2023:9).

Ahora bien, en los precedentes *Smith V. Maryland* como también *United States V. Miller*[33], se excluyó de los ámbitos de protección de la IV enmienda situaciones tales como la información que las personas exponen continuamente a *otras*. Cada uno abre su vida privada a otros individuos bajo su propio riesgo. Si se comparte información al público en general, no podríamos tener una expectativa de privacidad razonable (*reasonable expectation of privacy*) respecto de esos datos.

Véase este pasaje del voto de la jueza Sotomayor en el caso *United States v. Jones*:

> Las personas revelan una gran cantidad de información sobre si mismas a terceros en el curso de llevar a cabo tareas mundanas. Las personas revelan los números de teléfono que marcan o mensajes de texto a sus proveedores de telefonía móvil, las URL que visitan […] y los libros, comestibles y medicamentos que compran a los minoristas en línea.

Esta doctrina, creada a partir de los precedentes anteriormente mencionados, se lo conoce en los EE.UU. como "*Third-party doctrine*". Si bien estos casos no trataban sobre prueba OSINT y esta doctrina no fue incorporada aún en nuestro país, podríamos aplicar el mismo criterio en este tipo de elemento de juicio. El derecho a la intimidad solo se ve lesionado al violarse la expectativa de privacidad que tiene una persona por sus acciones. Existe una protección atenuada de la intimidad en tanto, cuando una persona "corre el velo" de su intimidad y permite que su información sea visualizada

[33] Xander de los Reyes (2023) "la doctrina del contenido especifico: el derecho a la seguridad en los efectos digitales", P. 9-10. "En el caso Smith V. Maryland, se creía que Michael Lee Smith había robado a una mujer. Las autoridades también sospechaban que llamaba continuamente a la víctima para acosarla por el robo. Para investigar, el gobierno solicitó a la compañía telefónica de Smith que instalara un "registro de llamadas", un dispositivo que registra los números marcados, pero no el contenido de las llamadas. Cuando los registros indicaron que Smith marcó el número de teléfono de la víctima, las autoridades lograron obtener una orden de registro para encontrar más pruebas. Smith fue posteriormente identificado por la víctima en una rueda de reconocimiento y condenado por robo. Argumentó que el registro violaba sus derechos amparados por la Cuarta Enmienda y apeló. En el caso Estados Unidos contra Miller, el gobierno acusó a Mitch Miller de no pagar el impuesto sobre el alcohol por el equipo de destilación. Para investigar, las autoridades federales citaron a dos bancos de Miller. Sin orden judicial, obtuvieron los registros de sus cuentas. Estos documentos se utilizaron posteriormente en su contra ante el tribunal, donde fue condenado. Miller apeló y argumentó que se violaron sus derechos amparados por la Cuarta Enmienda al obtener sus registros bancarios sin orden judicial. La Corte Suprema falló en contra de los demandantes en los casos *Miller* y *Smith*. Según la Corte, ambos hombres proporcionaron voluntariamente su información a terceros".

por otros, no puede luego alegar la violación de sus derechos constitucionales, cuando fue su propia conducta la que permitió que accedan a sus datos personales.

En este sentido, difícilmente se puede sostener una expectativa razonable de privacidad cuando se difunde contenido a través de redes abiertas como YouTube, Facebook o Instagram, donde la cuenta puede estar "abierta" para el acceso del público en general, sin necesidad de una "autorización" previa por parte del creador de la cuenta para ver el contenido.

Lo cierto es que, si el usuario posee un perfil "público", es claro que asume los riesgos que esto implica en cuanto a su privacidad, no solo implícitamente por su conducta, sino también al aceptar los términos y condiciones de las plataformas, que en la generalidad de los casos hacen mención a dicha problemática y posibles soluciones para resguardar la privacidad de los usuarios.

Ahora bien, esto no quiere decir que las garantías constitucionales previstas en nuestra carta magna no sigan vigentes en las redes, sino que, como en cualquier escenario tanto físico como virtual, los derechos no son absolutos, sino que son relativos y que algunos espacios gozan de una protección más fuerte que otros. Seguirá vigente la protección de la intimidad, pero esta sería de una manera "atenuada" en favor de la persecución del crimen y la seguridad ciudadana.

En consecuencia, podríamos sostener que, en algunos casos, la protección de la intimidad es menos intensa en razón de la propia decisión del usuario de exponer contenido ante terceros. Creo que en estos casos, razonablemente, podría no ser necesaria una regulación legal especifica, ni una autorización judicial para la recopilación de la información. Es más, si existe un "descorrimiento del velo" de la intimidad por parte de la persona investigada, no solamente no haría falta como requisito una autorización judicial previa, sino que tampoco sería necesario aplicar analógicamente las reglas procesales relativas a la vulneración de la intimidad, en tanto el ámbito de protección fue reducido por el propio usuario, quien voluntariamente expone su contenido a otros. En los restantes casos, sería deseable una regulación o, si se quiere, la aplicación analógica de las reglas procesales relacionadas con la invasión de espacios de intimidad, como podrían ser las de las intervenciones telefónicas —centralmente, la exigencia de autorización judicial previa—.

5 Conclusiones.

Ahora bien, a modo de conclusión de este trabajo, aquí se intentó demostrar los riesgos que implica la investigación sobre Fuentes Abiertas en un contexto donde la IA se encuentra en auge, vimos los problemas que pueden existir en un proceso penal en torno a la evidencia OSINT, pudiendo ser del tipo epistémicos como también normativos.

En cuanto a los problemas epistémicos, vimos que el juez suele otorgar una deferencia especial a lo que ve en las redes, sin preguntarse de antemano si lo que ve es real o no, aprendimos que apoyar la confianza de la prueba OSINT sin tomar los recaudos necesarios puede llevar al error, es decir, a la condena de un inocente o a la absolución de un culpable. A raíz de ello, propuse algunas medidas concretas, como algunos cuidados en la cadena de custodia del material como también la aplicación de códigos "hash" a la prueba digital. Asimismo, propuse la realización de un peritaje previo obligatorio bajo las reglas de las pruebas definitivas e irreproducibles, y también otras medidas más generales, relacionadas con la capacitación de los operadores del sistema, como son la celebración de convenios. También vimos la posibilidad de implementar un "consultor experto" o "*technical advisor*" "que pudiera educar básica y rápidamente al juez sobre las cuestiones más elementales" respecto a la IA y la prueba OSINT.

Ahora bien, en cuanto a los problemas normativos, se analizó la falta de previsión normativa de estas pruebas y, en conexión con ello, con la posible injerencia en ámbitos íntimos. Al respecto, se sostuvo que, si bien es deseable la regulación de esta clase de evidencias, no sería necesaria una autorización legal o judicial específica en aquellos casos en los que involucren injerencias *nimias* en la intimidad. Esto sería posible en el ámbito digital cuando son los propios usuarios quienes "descorren el velo de protección" de dichos ámbitos. En tal caso, dijimos que no es requisito una autorización judicial previa, como tampoco sería necesario aplicar analógicamente las reglas procesales relativas a la vulneración de la intimidad. En los restantes casos, donde existe una "expectativa razonable de intimidad" sería deseable una regulación o, si se quiere, la aplicación analógica de las reglas procesales relacionadas con la invasión de espacios de intimidad, como podrían ser las de las intervenciones telefónicas —centralmente, la exigencia de autorización judicial previa—.

En consecuencia, la prueba OSINT puede considerarse confiable, siempre que se tomen las precauciones del caso, y puede resultar de gran relevancia para resolver un conflicto penal. Desde el punto de vista epistémico, podría haber problemas si no se toman los recaudos necesarios mencionados previamente. Desde el punto de vista normativo, no es necesario un marco de regulación legal de este elemento de juicio, mientras no exista una "expectativa razonable de privacidad", mientras que si existe una "expectativa" es necesario que se aplique analógicamente las reglas procesales relacionadas con la invasión de espacios de intimidad, como el aplicable a las intervenciones telefónicas —centralmente, la exigencia de autorización judicial previa—. En tales casos, no habría impedimento por parte de los Magistrados para valorar este tipo de elemento de prueba.

6 Bibliografía.

SAMPSON, F. (2017). Intelligent evidence: using open source intelligence (OSINT) in criminal proceedings. Police Journal, 90(1), 55-69.

FERRER BELTRÁN, J. (2007). *La valoración racional de la prueba*, Madrid, Marcial Pons.

— (2022). Introducción. En FERRER BELTRÁN (coord.), *Manual de Razonamiento Probatorio*, Suprema Corte de la Justicia de la Nación de México, Ciudad de México, pp. 16-17.

TROTTIER, D. (2015). Coming to terms with social media monitoring: uptake and early assessment. Crime Media Culture, 11(3), 317-334.

GISSEL, V. (2019). *Artificial Intelligence and its impact on the fourth industrial revolution*: *a review*, Jornada Internacional de inteligencia Artificial & aplicaciones, *10*(6), 43.

LILIANA, M. (2025). *Inteligencia Artificial*, Hammurabi.

GASCÓN ABELLÁN, M. (2021). Ideas para un "control de fiabilidad" de las pruebas forenses. Un punto de partida para seguir discutiendo. En *Manual sobre derechos humanos y prueba en el proceso penal*, p. 66.

LAUDAN, L. (2013). *Verdad, error y proceso penal*, Madrid, Marcial Pons, traducción de Carmen Vázquez y Édgar Aguilera del original *Truth, Error and Criminal Law*, *Cambridge University Press*, 2006.

TARUFFO, M. (2008). *La prueba*, Madrid, Marcial Pons, traducción de Laura Manríquez y Jordi Ferrer Beltrán.

VELEDA, D. (inédito), (s.f.). *Apuntes sobre la relevancia y confiabilidad de la prueba*.

DEI VECCHI, D. (2019). "La no tan sana crítica racional", En Letra: Derecho Penal, 6(9), 37.

GONZÁLEZ LAGIER, J. D. (2003). Hechos y argumentos (racionalidad epistemológica y prueba de los hechos en el proceso penal) (II). *Jueces para la democracia*, (47), 35-50.

GASCÓN ABELLÁN, M. (2021). Ideas para un "control de fiabilidad" de las pruebas forenses. Un punto de partida para seguir discutiendo. *En Manual sobre derechos humanos y prueba en el proceso penal*, p. 51-81.

TERENCE, A. DAVID, S. WILLIAM, T. (2015). *Análisis de la prueba*, Madrid: Marcial Pons.

VÁZQUEZ, C. (2022). Presentación de la traducción al castellano del Informe del PCAST sobre la ciencia forense en los tribunales penales. *Quaestio facti. Revista Internacional sobre Razonamiento Probatorio*, (3), 275-480.

DUCE, M. (2018). Prueba pericial y su impacto en los errores del sistema de justicia penal: Antecedentes comparados y locales para iniciar el debate. *Ius et Praxis*, 24(2), 232-261.

HERDY, R. (2020). Ni educación, ni deferencia ciega. Hacia un modelo crítico para la valoración de la prueba pericial. *Discusiones*, *24*(1), 87–112. https://doi.org/10.52292/j.dsc.2020.2206.

VÁZQUEZ, C. (2020). El diseño normativo de las pruebas periciales, a propósito del razonamiento inferencial de los expertos y la comprensión judicial. *Discusiones*, *24*(1), 29–60. https://doi.org/10.52292/j.dsc.2020.2204.

GASCÓN ABELLÁN, M. (2020). Además de la verdad, defensa de los derechos cuando se buscan pruebas. En *El compromiso constitucional del iusfilósofo. Estudios en homenaje a Luis Prieto Sanchís* (pp. 178–201). Palestra.

VERA SÁNCHEZ, J. S. (2021). El principio de inclusión de la prueba relevante en el Código Procesal Penal chileno. *Revista Chilena de Derecho, 48*(1), 81-106. https://doi.org/10.7764/R.481.4.

DEI VECCHI, D. (2020). "Admisión y exclusión de pruebas: índice para una discusión". En Pensar la Prueba 1, editado por Pablo Rovatti y Alan Limardo. Buenos Aires: Editores del Sur.

VANINETTI, H. (2020). *Derecho a la Intimidad en la era digital*, Hammurabi.

CHAIA, R. A. (2025). *La prueba digital: Principios y garantías constitucionales para su aplicación en el proceso penal* (1.ª ed., 1.ª reimpresión). Hammurabi, José Luis Depalma Editor.

DE LOS REYES, X. (2023) la doctrina del contenido especifico: el derecho a la seguridad en los efectos digitales, 2 P.L.J. 5, P. 5-17.

PÉREZ BARBERÁ, G. (2015) "Reserva de ley, principio de legalidad y proceso *penal,* pp. 42-92.

PILARCHE, S. L. (2020). La prueba digital y su valor probatorio en el proceso penal. *Análisis de Derecho Penal y Procesal Penal - Revista de Doctrina y Jurisprudencia Penal*, (5), 1-22.

DELGADO DEL RINCÓN, L. E. (2012). Algunas consideraciones sobre la regla de exclusión de la prueba ilícita: Excepciones y eficacia. En A. Torres del Moral (Ed.), Constitución y democracia. Ayer y hoy: libro homenaje a Antonio Torres del Moral (Vol. 2, pp. 1515-1538). Editorial Universitaria Ramón Areces.

FIVECAST. (s.f.). *Beyond the buzzwords: AI in action for intelligence teams – How can AI enhance open-source intelligence?*.

https://www.fivecast.com/educational-resources/ebook-explore-the-role-of-ai-in-osint/.

HASSAN, N. A., & HIJAZI, R. (2018). *Open source intelligence methods and tools: A practical guide to online intelligence*. Apress.

https://doi.org/10.1007/978-1-4842-3213-2.

HANLEY, H. & DURUMERIC, Z. (2024). *Machine-Made Media: Monitoring the Mobilization of Machine-Generated Articles on Misinformation and Mainstream News Websites*.
https://doi.org/10.48550/arXiv.2305.09820.

CHUN CHU, K & DONG, J. (2024). *Misinformation and Literacies in the Era of Generative Artificial Intelligence: A Brief Overview and a Call for Future Research.*

https://doi.org/10.1177/27523543241240285.

United Nations Office on Drugs and Crime (UNODC). (2025). *Detect and respond: OSINT investigations*.

https://syntheticdrugs.unodc.org/syntheticdrugs/es/cybercrime/detectandrespond/investigation/OSINT.html.

UNESCO. (2019). *Estudio preliminar sobre los aspectos técnicos y jurídicos relativos a la conveniencia de disponer de un instrumento normativo sobre la ética de la inteligencia artificial (206 EX/42).*

https//unesdoc.unesco.org/ark:/48223/pf0000367422.

GOBIERNO DE ESPAÑA. (2023). *¿Qué es la inteligencia artificial (IA)? Plan de Recuperación, Transformación y Resiliencia.*

https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr.

MOYANO, N. (s.f.). *Deepfakes: el nuevo paradigma de la desinformación en las redes sociales y el derecho a la intimidad.*

https://www.hammurabi.com.ar/moyano-deepfakes/.

U.S. DEPARTMENT OF HOMELAND SECURITY. (2019). Increasing threat of deepfake identities.

https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

OFICINA DEL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS. (2020). El protocolo Berkeley ofrece orientación sobre cómo usar la información digital pública para luchar por los derechos humanos. Recuperado el 10 de junio de 2025.https://www.ohchr.org/es/stories/2020/12/berkeley-protocol-gives-guidance-using-public-digital-info-fight-human-rights.

7 Apéndice I. Reglas de actuación para los Magistrados ante la falta de regulación legal.

Ahora bien, a raíz de la falta de una regulación legal a la cuestión, pasare a exponer ciertas reglas que podrían orientar la actuación de los Magistrados. Podríamos decir que ya existe un marco regulatorio con respecto a las pruebas de fuentes abiertas. Es el "Protocolo Berkeley" publicado en marzo de 2024. Este protocolo fue creado por el Centro de Derechos Humanos de la Universidad de California, en Berkeley, y la Oficina de Derechos Humanos de las Naciones Unidas. Este protocolo se encarga de fijar lineamientos en el manejo de la evidencia proveniente de fuentes abiertas, y se creó con la finalidad de utilizarse en la investigación de violaciones a los Derechos Humanos en contexto de crímenes internacionales.

Entonces, "el protocolo Berkeley proporciona directrices, orientación sobre metodologías y procedimientos para la recopilación, análisis, y conservación de información digital de una manera profesional, legal y ética. También establece medidas […] con el fin de proteger la seguridad […] de testigos, victimas y personas" (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2020). Uno podría decir que el personal policial y judicial abocado a las tareas investigativas puede llevar a cabo sus labores ateniéndose a dicho protocolo[34]. En otros países esto es viable ya que los peritos informáticos se valen, en muchas ocasiones, de estándares internacionales; "los peritos informáticos, una vez que el material a examinar arriba a sus laboratorios […] ante la ausencia de normas locales sobre la materia. Se recurría al

[34] La Policía Federal Argentina, bajo la resolución 428/2024 del Ministerio de Seguridad con fecha de sanción 27 de mayo de 2024 estableció como debe ser la actuación del Personal Policial al investigar en fuentes abiertas, las fuentes policiales y de seguridad federales deberán adecuar su conducta a las siguientes pautas, principios, criterios, recomendaciones y directivas para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos. dichas tareas preventivas se llevarán a cabo únicamente mediante el uso de sitios web de acceso público y fuentes digitales abiertas, entendiéndose estas como los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implica una transgresión al derecho a la intimidad de las personas, conforme lo normado en la ley de protección de datos personales N° 25.326 y sus normas reglamentarias.

uso de facto de estándares técnicos de organismos internacionales adaptados, aplicados en otros países con mayor desarrollo y avance en la materia" (Pilarche, 2020, p. 1). Asimismo, existen recomendaciones internas, ya que se encuentra disponible la Guía de Obtención, Preservación y Tratamiento de la Evidencia Digital del Ministerio Público Fiscal de la Nación (en adelante, MPF). En caso de que el Juez a cargo de las actuaciones vea que la investigación no fue llevada adelante siguiendo lo establecido en el protocolo internacional o la guía de actuación del MPF, este puede asignarle un menor valor probatorio o directamente no valorar ese elemento de juicio a los fines de resolver la situación procesal del imputado.

En síntesis, si bien no existe una ley propiamente dicha que regule *OSINT*, si existe un protocolo como también una guía de recomendación dictadas ambas por organismos de prestigio que establecen recomendaciones de calidad para la investigación en fuentes abiertas. No debería existir ningún inconveniente por parte de las distintas judicaturas en lo relativo a su aplicación a los casos concretos que se presenten. Por lo que los organismos de la Justicia deberán atenerse al Protocolo de Berkeley o a la guía del MPF cuando exista evidencia proveniente de fuentes abiertas en aquellas causas penales que tramiten ante sus estrados.