HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

# Investigaciones abiertas para la construcción de evidencia

Diciembre 2025

# HEINRICH BÖLL STIFTUNG
## BUENOS AIRES
Argentina | Uruguay | Paraguay


La Fundación Heinrich Böll es la fundación política alemana cercana al partido Alianza 90/Los Verdes. Tiene su sede central en Berlín y actualmente cuenta con 34 oficinas en todo el mundo. En América Latina la fundación se siente especialmente comprometida, junto con muchas organizaciones socias y amigas, con la política climática, la promoción de la democracia y la justicia de género, así como con la consolidación institucional y profundización de los derechos humanos. Especialmente, en los contextos actuales, resulta fundamental defender y fortalecer sistemas de medios democráticos y el periodismo independiente, contra la manipulación deliberada por el uso masivo de fake-news y agresiones permanentes desde los poderes. Consideramos clave fortalecer a la sociedad civil en el dialogo permanente entre ciudadanía e institucionalidad política como práctica democratizadora. Hacemos especial hincapié en el intercambio de conocimientos y la comprensión entre actores en Europa y América Latina, para lo cual promovemos el diálogo internacional, esencial para la acción política constructiva.

HEINRICH BÖLL STIFTUNG
TECNOPOLÍTICA

# Investigaciones abiertas para la construcción de evidencia

Diciembre 2025


ARGENTINA HUMANA

EdIPo
Investigación Política

**Investigaciones abiertas para la construcción de evidencia**
Obra de distribución gratuita
Diciembre 2025
Publica Oficina Buenos Aires de la Fundación Heinrich Böll



**Autores**
Matthew Gillett | Wallace Fan | Facundo Cifelli | Luz Conde Vicente | Raisha Correa | Andrés Carbel | Joaquín Simbad Rapoport | Annick Aubert | Camila Palacin

**Coordinación editorial**
Valen Ave

**Equipo editorial**
Gabriela Kletzel | Raisha Correa | Andrés Carbel | Joaquín Simbad Rapoport

**Traducción**
Rizoma Traducciones (Rodra Castro y Nicolás Castrilli)
rizoma.trad@gmail.com

**Diagramación y Diseño Gráfico**
Marilyn Fernandez

**Imágenes de portada y artículos**
Clarote & AI4Media. Licencia CC BY-NC-SA 4.0.

**Ilustración "El método grillo: cómo reconstruir una verdad manipulada"**
Nicolás Daniluk. Todos los derechos reservados.

**Contacto**
info@ar.boell.org
ar.boell.org

# Índice

**Prólogo.....6**

**Introducción.....7**

**Prueba pericial y la información digital de fuentes abiertas.....9**

**El método Grillo: cómo reconstruir una verdad manipulada.....37**

**Violencia en redes sociales y retos de la evidencia digital: a propósito del caso Julia Mengolini.....42**

**Enfoques, estrategias y dificultades en el litigio de agresiones por parte de milicias digitales de ultraderecha.....59**

# Prólogo

La Fundación Heinrich Böll en Buenos Aires se propone contribuir con sus líneas de trabajo al fortalecimiento de la democracia y los derechos humanos en sus dimensiones sociales, politicas e institucionales, para lo cual el acceso a la información juega un rol fundamental en un contexto atravesado por profundas transformaciones tecnológicas. En ese marco, la investigación abierta y la construcción colectiva de evidencia constituyen una de las apuestas más ricas de la sociedad civil para enfrentar sus desafíos.

La acelerada digitalización de la vida social, la personalización en burbujas algorítmicas y el uso intensivo de sistemas de inteligencia artificial han reconfigurado el ecosistema informativo, generando nuevas oportunidades, pero también amenazas para la integridad de la información, el debate público, la confianza en las instituciones democráticas y los procesos políticos. Fenómenos como la desinformación, las *fake news* y los *deepfakes*, los ataques políticos coordinados mediante prácticas de *trolleo* y *doxeo*, potenciados por tecnologías cada vez más accesibles, sofisticadas y concentradas en manos de unos pocos tecno-conglomerados, en algunos casos culminan en una especie de intervencionismo político de alcance global, y desde luego tensionan los marcos tradicionales nacional e internacionales de derechos y libertad de expresión, exigiendo respuestas innovadoras tanto a nivel nacional como regional e internacional.

Frente a este escenario, apostamos por desarrollar una línea de trabajo **tecnopolítica** que permita analizar críticamente el impacto de estas tecnologías, y aportar insumos para el diseño de políticas públicas que protejan los derechos en entornos digitales. A través del trabajo conjunto con organizaciones, periodistas, academia e instituciones, este eje busca contribuir a una gobernanza democrática y transparente de la tecnología, centrada en las personas y orientada al interés público.

En este camino publicamos **Investigaciones abiertas para la construcción de evidencia** que reúne experiencias, metodologías y reflexiones desarrolladas por organizaciones y equipos que trabajan en la documentación, el análisis y la intervención frente a la violencia institucional y ataques en entornos digitales. Compila propuestas para la evaluación de expertos en la Corte Penal Internacional con experimentos locales de reconstrucción digital y aprendizajes extraídos del litigio estratégico con el objetivo de aportar herramientas que fortalezcan las capacidades y el impacto de la investigación ciudadana.

*Michael Álvarez Kalverkamp*
*Director*
*Fundación Heinrich Böll*
*Oficina Buenos Aires*

# Introducción

El dossier **Investigaciones abiertas para la construcción de evidencia** es fruto de un trabajo colaborativo desarrollado durante el 2025 desde el espacio de intercambio *ataques en entornos digitales* donde diversas organizaciones[1] buscamos retroalimentar procesos de investigación y litigio, sistematizar experiencias y metodologías que contribuyan al aprendizaje colectivo, y potenciar donde sea posible estrategias conjuntas de incidencia.

La publicación integra las experiencias locales de investigación–intervención del **Mapa de la Policía**, el **Equipo de Investigación Política** de la Revista Crisis y **Argentina Humana** con la traducción inédita de un artículo de **Matthew Gillet** y **Wallace Fan** para la Revista de la Justicia Penal Internacional (Oxford University Press). A lo largo de los textos se indaga en los aportes de la investigación ciudadana al terreno judicial, ya sea mediante reconstrucciones con datos extraídos de fuentes abiertas o coberturas colaborativas durante manifestaciones. Se resaltan la potencia y los desafíos técnicos, jurídicos y político-metodológicos de estas prácticas de intervención pública a través de la información recolectada y analizada de forma cooperativa.

Gillet y Fan en *Prueba pericial y la información digital de fuentes abiertas: llevar la evidencia en línea a los tribunales* proponen criterios para renovar los estándares de evaluación de experticia pericial por parte de la Corte Penal Internacional frente a los desafíos que representa para el paradigma exclusivamente individual, la naturaleza colectiva e interdisciplinaria de la investigación impulsada desde la sociedad civil con información digital de fuentes abiertas.

En *El Método Grillo: cómo reconstruir una verdad manipulada*, investigadores del Mapa de la Policía despliegan el paso a paso de la reconstrucción del atentado contra la vida del fotoperiodista Pablo Grillo producto del impacto de un proyectil de gas lacrimógeno durante una manifestación convocada por jubiladxs frente al Congreso. Se identificó la responsabilidad de un cabo de la Gendarmería Nacional que actuó fuera del protocolo que regula el uso de armas menos letales. Para ello fue necesario no solo los registros aportados por testigos desde distintos ángulos y el análisis de archivistas que cotejaron la información con la publicada por medios de comunicación, sino también el trabajo de físicos especializados para la realización de un peritaje técnico independiente a partir de la metadata acumulada y de artistas audiovisuales con capacidad de narrar los hechos de forma accesible, logrando una intervención en tiempo real con impacto sobre el relato oficial y proceso judicial.

*Violencia en redes sociales y retos de la evidencia digital: a propósito del caso Julia Mengolini* desarma el recorrido realizado por el Equipo de Investigación Política para aportar elementos a la causa judicial sobre la coordinación y complicidad institucional en el ataque orquestado contra la periodista feminista que incluyó d*oxeo, troleo, fake news* y *deep fake sexual*. Parten del caso considerado testigo para profundizar sobre los desafíos relativos a la investigación y producción de evidencia ante la complejidad de violencia política facilitada por la tecnología. A su vez, comparten herramientas y metodologías disponibles que invitan a multiplicar experimentos de investigación abierta para garantizar la transparencia y la rendición de cuentas.

---

Agradecemos especialmente los aportes de Amnistía Internacional Argentina, el Centro de Estudios Legales y Sociales (CELS), Fundación para el Desarrollo de Políticas Sustentables (FUNDEPS), Abogados y abogadas del Noroeste Argentino en derechos humanos y estudios sociales (ANDHES), Liberpueblo, Asuntos del Sur, DataGénero, Cooperativa Mover, Fundación Vía Libre, Argentina Humana y el Equipo de Investigación Política de la Revista Crisis.

Por último, *Enfoques, estrategias y dificultades en el litigio de agresiones por parte de milicias digitales de ultraderecha* recupera la experiencia y los aprendizajes de Argentina Humana en el litigio estratégico de ataques contra voces opositoras que tuvieron visibilidad pública. Ofrecen una sistematización de las distintas modalidades de violencia en línea y sus posibilidades de encuadre legal en el contexto argentino, las limitaciones de la intervención judicial y las responsabilidades de las plataformas intermediarias.

Desde perspectivas locales, internacionales y de legislación comparada, los artículos constelan un diálogo de saberes sobre los desafíos de las tecnologías no solo en relación a sus potenciales riesgos, sino también sus posibilidades de apropiación comunitaria que sin sacrificar rigurosidad ofrecen respuestas creativas e innovadoras. La expansión del acceso a redes y dispositivos móviles democratiza las capacidades de investigación y documentación ciudadana mediante las múltiples herramientas disponibles para buscar, registrar, verificar, archivar, conectar y comunicar.

Mientras el ruido inunda los sistemas ultrapersonalizados de alimentación informativa, no da lo mismo cualquier verdad. La evidencia abierta construida de forma reticular permite garantizar el acceso a información de interés público y disputar relatos ante el atropello institucional.

*Valen Ave*
*Diciembre 2025*

# Prueba pericial y la información digital de fuentes abiertas

## Llevar la evidencia en línea a la sala de audiencias

Matthew Gillett* y Wallace Fan**
Traducido por Rizoma Traducciones (Rodra Castro y Nicolás Castrilli)

## Resumen

La información digital de fuentes abiertas (DOSI por sus siglas en Inglés: "*Digital Open Source Information*") se ha convertido en una fuente significativa de evidencia para la Corte Penal Internacional ("la Corte") y otras jurisdicciones que aplican el derecho penal internacional. Sin embargo, su uso en los litigios plantea preguntas sobre quién puede ser considerado un perito en DOSI y qué métodos y salvaguardias deben adoptar. Este artículo examina cómo la Corte puede recibir DOSI mediante prueba pericial sin comprometer estándares rigurosos de determinación de hechos. Aborda los desafíos que la DOSI introduce en el paradigma del dictamen pericial, incluidos la ausencia de un sistema de acreditación general y formalizado de especialistas en DOSI, el carácter típicamente colectivo de las investigaciones basadas en DOSI y el riesgo de que interpretaciones erróneas y sesgos conduzcan a

*Profesor Senior (Profesor Asociado), Facultad de Derecho de la Universidad de Essex; titular de un mandato especial de las Naciones Unidas (Grupo de Trabajo sobre la Detención Arbitraria); e Investigador Principal de la Unidad de Verificación Digital de la Universidad de Essex. [matthew.gillett@essex.ac.uk]

**Ex Gerente de la Unidad de Verificación Digital, Universidad de Essex. [wallacecffan@gmail.com]

Los autores agradecen a Nema Milaninia por sus valiosas contribuciones. Las opiniones aquí expresadas pertenecen únicamente a los autores y no reflejan necesariamente las de ninguna otra persona u organización. Todos los sitios web citados fueron consultados por última vez el 27 de octubre de 2023.



Publicación en acceso anticipado el 27 de diciembre de 2023.

conclusiones equivocadas. Propone un novedoso marco de seis factores con el que la Corte podrá identificar qué especialistas en DOSI están lo suficientemente cualificados como para ser considerados peritos. Al mismo tiempo, destaca que los especialistas en DOSI deben utilizar metodologías transparentes, accesibles y replicables, con mecanismos de retroalimentación para el control de calidad, procesos de revisión por pares y controles de sesgos. El objetivo del artículo es facilitar el uso de pruebas de DOSI sobre delitos graves para resolver casos de crímenes atroces, teniendo en cuenta los estándares rigurosos de investigación de los hechos y respetando los derechos al debido proceso y a un juicio justo.

# 1. Introducción

> *Es evidente. A medida que la ciencia continúa transformando el mundo social, grandes cambios en la investigación fáctica aguardan a todos los sistemas de justicia. Dichas transformaciones podrían resultar tan trascendentales como aquellas que ocurrieron en el ocaso de la Edad Media, cuando las formas mágicas de prueba cedieron ante los prototipos de la tecnología probatoria contemporánea.*[1]

El uso de información digital de fuentes abiertas (DOSI)[2] plantea preguntas fundamentales sobre el marco normativo que regula a los peritos ante la Corte Penal Internacional ("CPI" o "la Corte"). En particular, la creciente presencia de la DOSI en los procedimientos de la CPI exige un examen riguroso de la definición, el rol y la metodología del experto o perito.[3] A diferencia de los testigos comunes,[4] los peritos pueden declarar sobre asuntos que no experimentaron de manera directa.[5] La función que desempeñan estos especialistas puede tener un impacto significativo en el resultado de un juicio, especialmente en casos internacionales donde puede ser difícil obtener evidencia tradicional de la escena del crimen.[6] Sin embargo, incluir DOSI en el enfoque que los tribunales internacionales aplican a la prueba pericial es problemático porque: (i) desafía la distinción binaria entre peritos y testigos legos; (ii) su ontología basada en el trabajo colectivo resulta incongruente con el paradigma tradicional del perito individual; y (iii) su naturaleza dinámica debe conciliarse con la necesidad de transparencia y replicabilidad.[7]

Para abordar la posible disonancia entre la DOSI y la prueba pericial, este artículo explora vías para que la Corte facilite la recepción de DOSI manteniendo, al mismo tiempo, estándares rigurosos de determinación de hechos. Examina cómo los especialistas en DOSI pueden mitigar los riesgos de que su trabajo sea considerado poco confiable o inadmisible. De forma destacada, propone un novedoso test de seis factores para designar a especialistas en DOSI como peritos.

La tesis central del artículo es que debe mantenerse una firme distinción entre peritos y testigos legos como parte de la estructura normativa de la Corte. Esto favorecerá la fiabilidad en la determinación de los hechos y reforzará la legitimidad de las decisiones de la CPI. Al mismo tiempo, se sostiene que la CPI (y otras instituciones que aplican el derecho penal internacional), junto con la comunidad DOSI, pueden ajustar sus metodologías de trabajo para apoyar la investigación y el enjuiciamiento de crímenes atroces. Los tribunales internacionales pueden incorporar la DOSI mediante el establecimiento de parámetros claros, objetivamente justificados, accesibles y no sesgados para reconocer a especialistas en DOSI como peritos. Por su parte, los especialistas en DOSI deben emplear metodologías transparentes, accesibles y replicables, con mecanismos de retroalimentación para el control de calidad, procesos de revisión por pares y controles de sesgo.

Este artículo ingresa a un tema de discusión novedoso al examinar el uso de la DOSI dentro del marco de la prueba pericial. Se diferencia de evaluaciones previas sobre prueba pericial en derecho internacional, que suelen centrarse en materiales probatorios más "tradicionales" presentados ante tribunales internacionales, como análisis de alineamientos locales (BLAST) e identificación mediante

ADN.[8] De manera similar, se distingue de estudios sobre la DOSI, que han tendido a centrarse en su valor probatorio *in abstracto*, sin analizar cómo sería introducida como prueba ante tribunales como la CPI. De hecho, varias publicaciones de referencia sobre el rol de la DOSI en casos de crímenes atroces omiten toda discusión relativa al dictamen pericial.[10] Por otro lado, los trabajos que sí abordan el dictamen pericial solo contienen análisis muy limitados de cómo podría aplicarse ese marco normativo a la DOSI. Incluso manuales ampliamente citados sobre DOSI, como el Berkeley Protocol on Digital Evidence, carecen de una evaluación detallada sobre la prueba pericial en este ámbito.[11]

Por el contrario, este artículo presenta una evaluación exhaustiva del marco normativo que regula la evidencia basada en DOSI y de los desafíos que plantea tanto para la CPI como para la comunidad DOSI. De manera significativa, realiza una contribución única a la literatura sobre justicia penal internacional al proponer un marco para determinar a quién se puede reconocer como perito en DOSI ante la CPI. El marco consta de seis criterios que reúnen orientaciones provenientes de la jurisprudencia, la doctrina y la experiencia.[12]

La formulación de este marco para la prueba pericial en DOSI constituye un recurso importante para que la Corte pueda tratar materiales de DOSI. Debido a que la DOSI suele recopilarse de manera remota por personas que no participaron en su creación,[13] será necesaria la evidencia de opinión para explicarla y verificarla, normalmente a través de un experto.[14] El uso del marco normativo que rige la prueba pericial ayudará a evitar la mala interpretación o el mal manejo de la DOSI.[15] También contribuirá a garantizar que el proceso cada vez más importante de[16] recopilación y presentación del material DOSI se realice legalmente y sin violar reglas procesales o protecciones de derechos humanos, ni perjudicar a terceros.[17]

La necesidad de examinar cómo puede presentarse la DOSI mediante prueba pericial también es importante para otras instituciones que aplican derecho penal internacional. En los últimos años, la sociedad civil ha intensificado sus labores de documentación y, con ello, el uso de materiales digitales en los procedimientos judiciales.[18] Además de la CPI, existen otras organizaciones internacionales que utilizan la DOSI como las misiones de determinación de hechos de la ONU,[19] organizaciones de derechos humanos, periodistas de investigación[20] y tribunales nacionales en casos de crímenes atroces bajo jurisdicción universal.[21] Garantizar que el marco normativo que regula la prueba pericial pueda incorporar la DOSI es esencial para ampliar el alcance de la justicia penal internacional.[22]

## 2. La creciente necesidad de abordar la DOSI en el contexto de la prueba pericial

La DOSI abarca una gran variedad de materiales, incluidos videos, fotografías, sitios web, imágenes satelitales, grabaciones de drones, registros de máquinas, transacciones financieras y documentos gubernamentales.[23] La generación, recolección y verificación[24] de la DOSI implican volúmenes enormes de material y son fenómenos digitales altamente dinámicos[25]: cada minuto se publican más de 350.000 tuits en Twitter (ahora "X"), y se cargan más de 500 horas de video en YouTube.[26] Mucho de este material se encuentra en formatos nunca antes analizados por tribunales internacionales. Y a pesar de lo novedoso de los avances procesales y de fondo que realizaron los tribunales *ad hoc* durante la década de 1990, estos se basaban mucho más en evidencia analógica que en evidencia digital.[27] En consecuencia, la CPI debe forjar su propio enfoque respecto de la DOSI, con muy pocos precedentes de jurisprudencia autorizada a los cuales recurrir para obtener orientación procesal.

Hasta ahora, han habido muy pocos casos, si es que existe alguno, en los que la CPI se haya basado en

DOSI para llegar a una determinación crucial.[28] Mientras que la DOSI desempeñó un papel central en el caso Al-Werfalli, este no avanzó a la fase de juicio debido a su presunta muerte mientras se encontraba en fuga.[29] En Lubanga, las Salas de Primera Instancia y de Apelaciones se apoyaron en videos, pero estos no parecen haber constituido DOSI en el sentido aquí empleado,[30] y sus aspectos técnicos no fueron objeto de análisis detallado.[31] La admisión y valoración, por parte de la Sala de Primera Instancia en Bemba, de grabaciones de medios de comunicación de *Radio France Internationale Journal Afrique*[32], fue revocada por la Sala de Apelaciones, que describió dicha prueba como "débil, compuesta a menudo por reportes de prensa que incluían rumores de fuente anónima".[33] En el caso por desacato *Bemba et al.*, la Fiscalía presentó fotografías de Facebook para demostrar la relación entre los participantes en el esquema de soborno, pero la Sala de Primera Instancia no se refirió explícitamente a dichas publicaciones en su fallo.[34]

La CPI ha tenido la oportunidad de abordar cuestiones relacionadas con DOSI, incluso en el contexto de prueba pericial, particularmente en los casos de Mali. Sin embargo, en *Al Mahdi*, la prueba pericial no fue impugnada, ya que las partes acordaron no presentar pruebas ni argumentos contrarios al acuerdo de declaración de culpabilidad.[35] En *Al Hassan*, un perito en análisis de video fue instruido por la Fiscalía para usar evidencia digital y plataformas como Google Earth para geolocalizar monumentos en la zona de Tombuctú, pero la sentencia no se había emitido al momento de redactarse este artículo.[36] En consecuencia, la Corte no ha tenido que enfrentarse al conjunto completo de desafíos procesales que puede plantear la DOSI.

Es imperativo que la Corte adapte sus procedimientos para atender los desafíos técnicos de la DOSI cuando se presenta como prueba. Las situaciones actualmente ante la Corte, como las de Libia, Ucrania y Palestina, prometen contener considerables cantidades de material DOSI. Por ejemplo, el mariscal libio Khalifa Haftar, quien supuestamente está siendo monitoreado por la CPI,[37] podría enfrentar la utilización de DOSI en un eventual caso en su contra para múltiples propósitos, incluidos demostrar las ejecuciones cometidas por su lugarteniente ya fallecido Mahmoud al-Werfalli,[38] mostrar sus propias declaraciones supuestamente ordenando que no se diera cuartel a prisioneros,[39] y probar la existencia de un conflicto armado. En tal caso, sería inevitable recurrir a peritos para verificar la autenticidad y fiabilidad de los materiales DOSI, incluso mediante geolocalización, cronolocalización, búsqueda inversa de imágenes y análisis de metadatos, tal como se discute en este artículo. En el contexto de Ucrania, distintas organizaciones de la sociedad civil han utilizado ampliamente materiales DOSI derivados de imágenes aéreas y satelitales[40]; la Comisión Internacional Independiente de Investigación sobre Ucrania ha citado declaraciones en línea del Kremlin[41]; y figuras influyentes han difundido declaraciones incendiarias mediante publicaciones en Telegram y otras plataformas[42], lo cual podría servir de base para imputaciones de incitación al genocidio y persecución. Ya se han planteado cuestiones de accesibilidad y equidad derivadas del uso de dichos materiales,[43] lo que probablemente conducirá al involucramiento de especialistas en DOSI como peritos. De manera similar, el actual conflicto entre Hamás e Israel ha generado un torrente de materiales DOSI que se han difundido ampliamente, incluidos videos del ataque del 7 de octubre de 2023 en el festival de música Nova, entrevistas con atacantes de Hamas detenidos y grabaciones de misiles y cohetes lanzados por ambas partes. Cualquier caso que surja de estos enfrentamientos involucrará una proporción significativa de materiales de tipo DOSI, que en muchos casos habrán sido vistos y compartidos masivamente y, algunos de ellos, alterados en línea, lo que nuevamente hará necesaria la participación de expertos en DOSI para analizar y verificar su contenido y procedencia. Asimismo, en los procedimientos judiciales que puedan derivarse surgirán controversias procesales sobre los parámetros de la prueba pericial, incluida la determinación de quién puede calificar como perito.

El marco de seis factores propuesto en este artículo para designar expertos en DOSI[44] puede ayudar en estas situaciones y en otras con un fuerte componente de DOSI. Aunque la adopción formal de este marco

corresponde a la Asamblea de los Estados Parte o a la Corte (dependiendo del instrumento en que se incorpore),[45] las Salas y las organizaciones pueden utilizar los criterios como guía en su trabajo actual sobre casos emergentes, sobre todo en tareas especializadas de recopilación, análisis y verificación de materiales DOSI.

Bajo los procedimientos actuales de la Corte, resulta preocupante la ausencia de un marco normativo establecido que regule específicamente la admisión de DOSI. El potencial uso indebido de la DOSI es cada vez más amplio y sofisticado. La tecnología moderna puede producir falsificaciones indistinguibles de material real al ojo humano.[46] En 2022, se difundió en redes sociales un video *deepfake* del presidente ucraniano Volodymyr Zelensky llamando a sus tropas a rendirse ante fuerzas rusas.[47] Otras imágenes publicadas por medios internacionales parecían mostrar a monjes budistas quemando víctimas rohinyás, pero en realidad mostraban la cremación de víctimas del terremoto de China de 2010.[48] Los riesgos de una confianza indebida en la DOSI pueden exacerbarse cuando la tecnología es nueva y visualmente impresionante, como la tecnología de reconstrucción digital.[49]

La detección de materiales DOSI falsos o manipulados requerirá cada vez más análisis especializados.[50] Esto incluye revisiones exhaustivas de metadatos y búsquedas inversas de imágenes, así como herramientas y técnicas más sofisticadas.[51] El análisis de materiales DOSI corresponde preferentemente a personas con habilidades y conocimientos especializados en este ámbito, quienes pueden declarar sobre su procedencia, fiabilidad y autenticidad.[52] Estas personas normalmente serían presentadas como expertos, especialmente porque no descubrieron originalmente los materiales DOSI, sino que participaron en su verificación e interpretación. En este sentido, resulta pertinente examinar si el marco procesal de la CPI que regula la prueba pericial es adecuado para aplicarse a la DOSI.

# 3. El marco procesal minimalista de la CPI respecto de la prueba pericial y la DOSI

## A. Prescripciones normativas pertinentes para la prueba pericial

Siguiendo los precedentes históricos de regímenes probatorios "menos estrictos" en procesos por crímenes de guerra,[53] el marco procesal de la CPI es flexible y de carácter abierto.[54] Este enfoque minimalista y flexible es particularmente notable respecto de la prueba pericial, en contraste con prescripciones más detalladas aplicadas en algunos sistemas nacionales.[55]

La cuestión fundamental es quién puede calificar como experto.[56] En Ntaganda, la Corte recurrió a la jurisprudencia del Tribunal Penal Internacional para la ex-Yugoslavia (TPIY) para definir al perito como "una persona que, en virtud de conocimiento, habilidad o formación especializada, puede ayudar al tribunal a comprender o determinar una cuestión de naturaleza técnica que se encuentre en disputa".[57] Poder determinar si una persona tiene suficiente pericia depende de su formación, experiencia en el campo pertinente, publicaciones y antecedentes adicionales relacionados con el tema sobre el cual declararía.[58] A pesar de este marco amplio, el rango de personas reconocidas como peritos ante la CPI y otras instituciones internacionales ha tendido a concentrarse en categorías tradicionales de valoración científica. El formulario de solicitud para la Lista de Peritos de la CPI incluye categorías como: balística; finanzas (investigaciones financieras/congelamiento de activos); medicina forense; grafología; psicología; reparaciones; así como experiencia específica sobre historia; sistemas judiciales; ciencia militar; policía; política y geopolítica; y lingüística.[59] No existe una mención explícita de la

DOSI ni de sus subcategorías.[60] Aunque personas en ámbitos no enumerados, como la DOSI, pueden solicitar inclusión en la Lista de Peritos, deben "explicar de qué manera su pericia es relevante para los procedimientos de la CPI".[61]

La jurisprudencia de los tribunales internacionales ha establecido parámetros para la presentación de prueba pericial. Fundamentalmente, los peritos pueden proporcionar opiniones sobre cuestiones más allá de su experiencia directa sensorial.[62] Pueden comentar sobre evidencia, abordando factores no inmediatamente aparentes (las características evidentes pueden ser transmitidas por testigos legos que ofrecen declaraciones de carácter sumario).[63] Es importante destacar que la prueba pericial debe versar sobre aspectos ajenos al conocimiento típico de una persona lega.[64] Esto justifica que el perito pueda proporcionar opiniones como evidencia y refleja la "naturaleza epistémica especial" del perito en litigios.[65] A la luz de este rol especial, la jurisprudencia de la CPI ha establecido que los peritos deben brindar su evidencia con la "máxima neutralidad y objetividad".[66]

En cuanto al contenido, la pericia del especialista debe cubrir la materia de la prueba que se pretende presentar.[67] En teoría, los peritos no deben pronunciarse sobre cuestiones últimas de hecho o derecho que son objeto de controversia y que corresponden al tribunal.[68] Deben excluirse las pruebas periciales que sustituyan las funciones del tribunal como, por ejemplo, opiniones sobre la culpabilidad o inocencia del acusado, o sobre la concurrencia de los elementos contextuales, materiales o mentales del delito.[69] En el Tribunal Penal Internacional para Ruanda (TPIR), esta prohibición condujo a la exclusión de las opiniones del Dr. Bernard Lugan sobre la "planificación del genocidio, la legitimidad de la defensa civil y evidencia relativa a la conducta del acusado".[70] Sin embargo, la regla admite interpretaciones. En otros casos, se ha permitido que peritos declaren sobre cuestiones que esencialmente equivalen a elementos del delito.[71]

Procesalmente, los peritos suelen presentar un informe que detalla su metodología y conclusiones, el cual se comunica a la otra parte con suficiente antelación al dictamen del experto. El contenido del informe y el dictamen propuesto deben corresponder a la pericia del experto y la evidencia debe ser potencialmente útil para el tribunal.[72] Los jueces de la CPI pueden, *proprio motu*, ordenar que se presente un informe pericial y que el perito declare.[73] También pueden ordenar informes periciales conjuntos[74] y disponer que peritos declaren simultáneamente.[75] De esta manera, el tribunal puede controlar el modo de instrucción de los expertos, la manera en que presentarán sus pruebas y los plazos para preparar y notificar sus informes.[76] Si bien el enfoque tenía por objeto ampliar la función judicial en la instrucción de los expertos,[77] en la práctica las partes han instruido a los peritos en muchos de los casos vistos hasta la fecha, tal y como se expone en el presente documento.

## B. El tratamiento de la DOSI bajo el marco normativo de la CPI

Aunque el marco de la CPI contiene escasa regulación directa sobre la DOSI, su jurisprudencia ha formulado orientaciones generales relevantes, como exigir que las partes indiquen la fecha y el lugar desde los cuales obtuvieron los materiales de fuentes abiertas.[78] También existe apoyo judicial y académico a la verificación de la DOSI en cuanto a su procedencia, metadatos, posibles manipulaciones,[79] atribuciones erróneas y autoría,[80] y autenticidad.[81] Establecer estos (contra)indicios de fiabilidad será importante para la presentación/admisión y valoración de la DOSI.

La DOSI contendrá con frecuencia prueba de oídas. La CPI ha mostrado considerable reticencia en admitir materiales abiertos basados en testimonios anónimos de oídas,[82] como los provenientes de ONG, Naciones Unidas y medios de comunicación.[83] Este escepticismo refleja preocupaciones sobre las

condiciones en que normalmente se recibe dicha prueba: sin juramento, sin posibilidad de contrainterrogar respecto de memoria, percepción, sinceridad y significado, y sin posibilidad de observar la conducta del declarante.[84] En relación con esto, la regla de la mejor prueba, que ha sido aplicada por los tribunales internacionales,[85] establece que "la Sala de Primera Instancia se basará en la mejor prueba disponible según las circunstancias".[86] En el caso de la DOSI, en los que a menudo existen múltiples copias de un elemento o publicación, a veces amplificadas con ajustes y material ajeno añadido, a la Corte le será de utilidad en sus deliberaciones que las partes procuren presentar la versión "original" más autorizada de la prueba.

Aparte de esas orientaciones generales y no específicas sobre la DOSI, hasta la fecha la CPI no ha adoptado ninguna norma jurídica específica (en el sentido formal del artículo 21) relativa a la recopilación, conservación, admisibilidad y verificación de la DOSI.[87] A falta de una regulación jurídica detallada de la DOSI, las pruebas periciales serán especialmente importantes para su autenticación e interpretación.

Una cuestión subyacente importante se refiere a la categorización taxonómica de la DOSI. Algunos comentaristas clasifican la DOSI como pruebas documentales,[88] otros como pruebas reales[89] o incluso como una combinación de ambas.[90] Al mismo tiempo, las opiniones de los expertos sobre la DOSI pueden considerarse pruebas testimoniales.[91] Esta terminología dispar pone de relieve la necesidad de claridad conceptual en relación con la DOSI.

La DOSI típica, como los videos o las fotos, implica decisiones editoriales, como mínimo en el sentido de determinar dónde enfocar la cámara y cuándo comenzar y terminar de capturar las imágenes o el video que se muestra.[92] Si bien dichos elementos podrían presentarse como pruebas documentales o pruebas reales, lo más probable es que se presenten como pruebas documentales, ya que se presentarán para demostrar la veracidad de su contenido más que su existencia y características físicas.[93]

La categorización probatoria de la DOSI es particularmente importante para determinar el papel de la prueba pericial. Si las imágenes o videos son evidencia material que "habla por sí misma",[94] el rol del perito se limitaría lógicamente a aspectos de verificación y autenticidad. Sin embargo, si la DOSI constituye prueba documental, entonces se requerirá el dictamen del perito para explicar e interpretar la evidencia, incluido su contenido, frente a los juzgadores. Esto implica un análisis caso por caso. Lo que sí está claro es que, cuanto más relevante sea el contenido de la DOSI desde un punto de vista forense, más probable será que las partes disputen su veracidad o la manera en que ha sido editada. Resolver estas cuestiones requerirá pruebas técnicas como "geolocalización, cronolocalización, verificaciones de coherencia interna dentro de un video y análisis de fuentes, verificaciones de consistencia entre múltiples elementos que supuestamente representan el mismo evento, y otros métodos *ad hoc*".[95] Estas tareas normalmente exceden la experiencia típica de una persona lega.[96] En consecuencia, la presentación de DOSI a menudo requerirá una opinión pericial, ya que "deben excluirse las cuestiones de opinión personal o de pericia fuera del ámbito de un testigo fáctico".[97]

El panorama anterior demuestra que las reglas y jurisprudencia de la CPI no se ajustan adecuadamente a los materiales DOSI en litigio, revelando vacíos e inconsistencias incluso a nivel taxonómico, y que estas tensiones solo aumentarán conforme crezca el potencial de manipulación de materiales digitales. Es imperativo abordar los desafíos que la DOSI plantea para el régimen de prueba pericial de la CPI, dadas la amplia accesibilidad y creciente prevalencia de materiales digitales en litigios sobre crímenes internacionales.[98]

# 4. Desafíos al paradigma establecido que rige la prueba pericial

## A. La DOSI pone a prueba la distinción binaria entre peritos y testigos legos

La accesibilidad y el carácter democratizador de la DOSI plantean desafíos a la actual distinción entre expertos y testigos legos.[99] En relación con una forma novedosa de pericia (el análisis acústico), el juez Lord Justice Bingham observó en el caso inglés *R v. Robb*:

> *"el riesgo de que, en un caso penal, a la Fiscalía se le permita llamar a un experto insuficientemente cualificado y la carga de la prueba de alguna manera se transfiera, y por ello recaiga sobre el acusado la obligación de rebatir un caso que jamás debería haber llegado ante el jurado... no hay manera justa de obligar a un acusado a enfrentar evidencia de opinión que presente un farsante, un charlatán o un aficionado entusiasta..."*.[100]

La referencia de Lord Bingham a los "aficionados entusiastas" tiene particular relevancia para la evidencia basada en DOSI. El fácil acceso a las herramientas y al material subyacente significa que no se necesita ninguna cualificación para comenzar a realizar investigaciones DOSI. El reconocido especialista en DOSI Eliot Higgins ha sostenido que "cualquiera puede realizar el análisis de información de fuentes abiertas (OSI, *Open Source Information*); es fácil aprender a hacerlo".[101] Él mismo es un "autodidacta que abandonó sus estudios universitarios".[102] En consecuencia, los participantes van desde expertos de renombre hasta estudiantes universitarios sin experiencia previa ni pericia técnica particular.[103] En este sentido, las características inclusivas y democratizadoras de la DOSI no encajan del todo con la categoría de perito, la cual tradicionalmente se ha basado en un nivel de habilidad o conocimiento especializado más allá del alcance típico de una persona lega o incluso de un juez.[104] A medida que una proporción creciente de la sociedad se vuelve digitalmente alfabetizada y competente en el uso de computadoras, será cada vez más difícil sostener que las formas básicas de verificación digital constituyen un tipo de conocimiento especializado que excede las capacidades normales de los juzgadores.[105]

Al determinar qué tipo de conocimiento especializado será aceptado como prueba pericial para materiales DOSI, resulta instructivo examinar ejemplos de especialistas en materiales audiovisuales que han sido reconocidos como peritos ante la CPI.

Estos especialistas acostumbran utilizar una variedad de técnicas de análisis con respaldo estadístico para sus conclusiones y/o con certificaciones o pertenencia a organismos profesionales ampliamente reconocidos.

Por ejemplo, en el caso *Al Hassan* ante la CPI, un perito en autenticación de voz comparó los elementos objeto de examen (que supuestamente contenían clips del acusado hablando) con elementos de referencia provenientes de sus comparecencias ante el tribunal.[106] Aunque normalmente se divulgan los CV de los expertos,[107] el CV de este perito no fue publicado. No obstante, él declaró tener diez años de experiencia en el área y haber asistido a sesiones de grupos de expertos de la *European Network of Forensic Science Institutes* (Red Europea de Institutos de Ciencias Forenses) sobre reconocimiento de voz.[108] Señaló que sus análisis incorporaban software altamente técnico, incluido un sistema automatizado de comparación de voz basado en algoritmos, el cual tomaba en cuenta el contexto acústico y la variabilidad entre momentos de habla, y generaba razones de verosimilitud respecto de la coincidencia entre los elementos examinados y los de referencia.[109] Por su naturaleza aparentemente basada en fundamentos científicos

y estadísticos, este tipo de evaluación es análoga a la prueba pericial tradicional, como puede serlo el análisis de correspondencia de ADN.

Otro ejemplo de habilidades especializadas consideradas suficientes para calificar como perito es el de la Oficial Forense de la CPI Amy Hak, quien fue llamada como experta en análisis forense de video en el caso *Al Hassan*.[110] Además de establecer sus funciones profesionales relacionadas con el análisis de video, su CV incluía referencias a su experiencia previa como experta en múltiples jurisdicciones como Canadá, detalles de las numerosas capacitaciones que había realizado y su certificación como analista forense de video.[111]

Más allá del alto grado de habilidad técnica involucrado en las evaluaciones de estos expertos, su certificación y/o pertenencia a organismos profesionales indica que contar con cualificaciones reconocidas por la industria aumenta la probabilidad de ser reconocido como perito. Esto también se desprende del formulario de solicitud para integrar la lista de expertos de la Corte, el cual pregunta si el solicitante está inscrito en un organismo profesional de su jurisdicción y si cuenta con un seguro profesional.[112]

En este sentido, cabe destacar que no existe una cualificación o certificación general en DOSI que tenga reconocimiento formal a nivel nacional o internacional equiparable, por ejemplo, al título de médico o patólogo forense.[113] Algunas organizaciones prominentes vinculadas a la justicia internacional ofrecen formación profesional en DOSI,[114] y en los últimos años se desarrollaron más cursos académicos en este campo.[115] Muchas entidades privadas ofrecen certificación en DOSI en el contexto de la ciberseguridad.[116] Sin embargo, dichos cursos aún no reciben un reconocimiento formal por parte de estructuras estatales que equivalga al de organismos reguladores establecidos, como los colegios nacionales de abogados o las juntas médicas. La ausencia de un sistema formal de cualificación que abarque el ámbito de DOSI dificultará que los jueces determinen quién puede ser considerado un perito DOSI.

En ausencia de un sistema de cualificaciones formales, una opción sería reducir el umbral de experiencia requerida y prescindir de cualquier exigencia de certificación. Ello permitiría aceptar de manera amplia a investigadores y entusiastas de DOSI como expertos. En algunas jurisdicciones internas, se ha ampliado el alcance de la prueba pericial aceptada para abarcar áreas más allá de las disciplinas científicas establecidas, incluidas "huellas dactilares, grafología y reconstrucción de accidentes ... el valor de mercado de tierras, barcos, cuadros o derechos ... la calidad de mercancías, o el mérito literario, artístico, científico u otro de obras presuntamente obscenas".[117] Permitir que los especialistas en DOSI ingresen al "club de los expertos" respetaría este mismo espíritu progresista.

No obstante, ampliar los parámetros puede reducir la calidad de los análisis y exacerbar los cuestionamientos sobre la selectividad al determinar quién es un experto. Ya se han planteado dudas sobre la subjetividad del proceso, que se ha descrito como "esencialmente subjetivo, con juicios normativos formados sobre la base de la educación, experiencia y otros antecedentes del perito, y a menudo, del volumen de canas en su cabeza".[118] Por ejemplo, ante el TPIR, "el experto propuesto, Jean Rubaduka, no fue calificado como perito en derecho constitucional ruandés, a pesar de que era miembro del tribunal constitucional y del consejo de Estado de Ruanda, y había enseñado derecho en la Universidad Nacional de Ruanda".[119] Asimismo, "un académico que enseñaba sobre Ruanda en la *School of African and Oriental Studies* (Escuela de Estudios Orientales y Africanos, SOAS) de Londres no fue calificado como experto", debido a que "carecía de un doctorado en la materia, trabajaba a tiempo parcial como optometrista, nunca había realizado investigación de campo en Ruanda y las revistas en las que había publicado carecían de prestigio".[120] Al mismo tiempo, otros tribunales han calificado como expertos a individuos únicamente sobre la base de su profundo conocimiento del tema, sin las certificaciones formales que tradicionalmente se ha requerido para esta categoría.[121]

Para evitar alimentar acusaciones de trato dispar y selectividad sesgada, será importante que la Corte establezca criterios objetivamente justificables para la calificación de expertos. Este paso hacia criterios objetivos refleja un cambio más amplio: dejar de otorgar el estatus de experto a un grupo reducido de individuos a menudo privilegiados sobre la base de evaluaciones relativamente opacas, y comenzar a reunir un conjunto de criterios más accesibles que cualquier persona pueda cumplir si demuestra habilidades y/o conocimientos suficientemente especializados. Los criterios objetivos también ayudan a evitar cualquier "distinción adversa fundada en motivos tales como género, edad, etnia, color de piel, idioma, religión o creencias, opinión política o de otra índole, origen nacional, étnico o social, posición económica, condición de nacimiento u otra condición".[122] Con estos fines, más adelante se presentan seis criterios que podrían emplearse para discernir quién puede calificar como experto en DOSI.[123]

## B. La DOSI como forma de recopilación colectiva de información

El perito suele imaginarse como un individuo ilustrado que, desde el estrado, instruye a los jueces o al jurado acerca de una cuestión técnica compleja en la que posee años de experiencia.[124] El lenguaje de la jurisprudencia de la CPI refleja este estereotipo,[125] refiriéndose a "un solo experto, imparcial y debidamente calificado".[126] Incluso el formulario de solicitud de la CPI para inscribir a organizaciones como expertas (que, en teoría, permite reconocer la actividad pericial de grupos ante la Corte) solicita explícitamente el "nombre de la persona designada para representar a la organización experta".[127]

La DOSI pone a prueba ese paradigma centrado en el individuo. Con frecuencia, la recopilación la hacen grupos multidisciplinarios compuestos por personas con distintos niveles de pericia y experiencia, trabajando de manera colaborativa.[128] Son múltiples los actores que a través de diversas plataformas pueden recolectar y verificar DOSI.[129] Esta actividad colectiva y colaborativa impone una carga significativa al investigador principal, quien debe garantizar la coherencia y las normas y procedimientos generales que aplique el equipo. Cuando existe colaboración entre organizaciones de la sociedad civil,[130] o entre entidades estatales y voluntarios individuales (por ejemplo, la identificación de los participantes en el asalto al Capitolio del 6 de enero),[131] o entre organizaciones internacionales y voluntarios individuales (como la campaña *Trace an Object* de Europol),[132] se agudiza el riesgo de enfoques inconsistentes.

El hecho de que la DOSI sea, por lo general, generada colectivamente no constituye un obstáculo absoluto para su admisión *qua* prueba pericial.[133] La pregunta inmediata que surge es quién, dentro del equipo colaborativo, debe fungir como experto y quiénes como testigos.[134] En situaciones análogas, un solo miembro del equipo ha declarado como experto mientras que otros han brindado testimonio fáctico.[135] Sin embargo, se requiere cautela: si el experto se incorporó al proyecto *ex post facto*, la parte contraria tendrá sólidos argumentos para objetar su declaración, alegando que no puede examinar de manera completa los posibles errores y sesgos de otros integrantes del equipo.

Sea cual sea el método de selección, la parte litigante debe instruir al designado como "experto" (o expertos) para realizar personalmente los análisis o supervisarlos. Si la parte litigante requiere ayuda adicional, debe instruir al experto para identificar explícitamente a toda persona que haya contribuido, detallar su aportación, e incluir sus CVs.[136] Durante el contrainterrogatorio, el perito podrá ser interrogado sobre las personas que lo asistieron en sus experimentos o análisis y deberá mencionar en su informe pericial el nombre de cualquiera de esas personas.[137] En el derecho del Reino Unido, por ejemplo, los expertos están obligados a incluir en sus informes no solo sus propias cualificaciones y las instrucciones recibidas, sino también "[i]nformación relativa a quién ha realizado mediciones, exámenes, pruebas, etc., así como la metodología utilizada, y si dichas mediciones, etc., se realizaron bajo la supervisión del perito'.[138] Bajo ninguna circunstancia debe el experto intentar presentar el trabajo de otras personas

como si fuera suyo sin el debido reconocimiento.[139] El equipo de DOSI también debe tener presente que, una vez iniciado el dictamen, el o los miembros designados no podrán comunicarse con el resto del equipo (salvo que la Corte otorgue un permiso excepcional). En un caso nacional reciente, el tribunal criticó explícitamente a un experto que, tras haber prestado juramento, llamó a varias personas fuera de la sala de audiencias para discutir cuestiones sobre las cuales estaba siendo interrogado.[140]

La composición de un equipo de DOSI será particularmente impugnable durante el juicio si el investigador principal, o cualquier otro miembro del equipo, está afiliado a una de las partes en litigio. Tal afiliación no constituye una prohibición absoluta; en el caso Al-Hassan ante la CPI se presentó, durante el proceso, el informe de Amy Hak, entonces Oficial Forense de la Fiscalía.[141] Asimismo, varios analistas de la Fiscalía han testificado en procedimientos ante el TPIY.[142] Sin embargo, algunos jueces lo consideraron inapropiado, como ocurrió cuando se rechazó el informe militar de Philip Coo en el caso Milutinović et al. debido a su posición como integrante del personal de la Fiscalía.[143]

El modelo de experto único entraría en conflicto con la tendencia democratizadora de la investigación colaborativa en DOSI, señalada anteriormente. Es poco probable que una sola persona posea todo el conocimiento necesario para testificar de manera exhaustiva acerca de una investigación completa de DOSI.[144] Por ejemplo, los investigadores de violaciones de derechos humanos contra la población rohingya han utilizado tanto imágenes satelitales como publicaciones en redes sociales para confirmar que las fuerzas militares de Myanmar saquearon e incendiaron sus aldeas.[145] Un experto en imágenes satelitales podría mostrarse reacio a testificar también como experto en publicaciones de redes sociales. Apegarse a un modelo de experto único podría perjudicar la eficiencia de una investigación de DOSI, ya que, al canalizar toda la información a través de una sola persona, se generan cuellos de botella en el análisis y la toma de decisiones. Por estas razones, los tribunales internacionales deben mostrarse receptivos a permitir que más de un miembro de un equipo de DOSI testifique sobre su función y hallazgos especializados, o que un solo miembro testifique pero que se reconozca que dicho perito no habrá realizado cada función que produjo los hallazgos del equipo, y que quizás solo actuó en un rol de revisión. En términos doctrinales, esto implica que la prueba pericial revestirá la naturaleza de una opinión, en lugar de una narración de experiencias directas.[146] Categorizarla como una opinión aumenta la necesidad de adoptar estándares rigurosos de revisión y transparencia dentro de los equipos de DOSI, como se expone en el presente trabajo, y exige que la Corte examine estos aspectos con especial atención al recibir y valorar la prueba pericial.

En suma, la naturaleza colaborativa de los proyectos de DOSI presenta oportunidades para que los tribunales internacionales se beneficien a partir de materiales altamente probatorios, pero exige ajustes al modelo tradicional de experto único. Si bien este cambio puede parecer radical para tribunales acostumbrados al modelo de experto único, refleja una evolución más profunda en los procedimientos judiciales (y en la sociedad en general), que se aparta de la idea de que el conocimiento especializado reside únicamente en individuos de alto estatus, y favorece en cambio que los proyectos altamente técnicos sean desarrollados de manera colaborativa por equipos de personal especializado.

## C. DOSI introduce riesgos elevados de error y sesgos conscientes o inconscientes

El uso de DOSI en procesos judiciales conlleva riesgos elevados porque los materiales audiovisuales pueden ser altamente persuasivos, pero puede que hayan sido recopilados de manera selectiva, ya sea consciente o inconscientemente. Estos riesgos se ven agravados por la naturaleza colectiva de las investigaciones DOSI, en las que las vulnerabilidades pueden multiplicarse. Además, la presentación de DOSI como prueba implica una transición desde un modelo de justicia crisol (centrado lo más

estrechamente posible en las cuestiones controvertidas y en la comparecencia de los testigos ante los jueces para evaluar su credibilidad),[147] hacia un enfoque más flexible, con múltiples y diversos puntos de verificación de la verdad (algunos de los cuales pueden ocurrir fuera de cualquier marco diseñado para garantizar la fiabilidad).[148]

Debido a ello, es particularmente importante que se adopten metodologías transparentes, accesibles y defendibles en las investigaciones DOSI.[149] En particular, los equipos de DOSI deberían establecer procesos de revisión, mediante los cuales los miembros con más experiencia supervisen el trabajo del equipo para asegurar su calidad y coherencia. Además de respetar el principio de No Hacer Daño,[150] debe adoptarse un proceso en bucle, en el que la información relativa a los enfoques, estándares y hallazgos pertinentes sea revisada, evaluada y devuelta a los miembros del equipo.[151] Tales metodologías rigurosas son esenciales para reducir el riesgo de que errores y sesgos permanezcan sin ser detectados ni cuestionados.[152]

Al examinar la práctica de presentación de prueba pericial en la justicia penal internacional se pueden elucidar los elementos de una metodología rigurosa. Los expertos deben recibir instrucciones claras de la parte que los propone (o la Corte), las cuales deben ser explicadas junto con su metodología en el informe pericial.[153] En Al Hassan, a la experta en análisis de video se le proporcionaron imágenes para geolocalizar y material de referencia con el cual compararlas. Sin embargo, las instrucciones de la Fiscalía también permitían que la experta recurriera a "cualquier otro medio" en caso de tener "problemas" al realizar la geolocalización.[154] Las instrucciones no precisaban si esos "otros medios" incluían la búsqueda de imágenes o materiales, y, de ser así, si tales búsquedas debían conservarse y documentarse. Ese tipo de omisión es potencialmente perjudicial, dado que los materiales pueden desaparecer de internet,[155] y considerando que la defensa puede tener interés en intentar replicar las búsquedas para identificar posibles puntos controvertidos.

En cuanto a la transparencia y accesibilidad, una parte debe garantizar que "las fuentes utilizadas en apoyo de cualquier declaración de un perito sean claramente indicadas y fácilmente accesibles para la otra parte, previa solicitud", de forma que la parte contraria pueda cuestionar el valor probatorio de dicha evidencia.[156] El incumplimiento de este requisito puede afectar el peso que los jueces estén dispuestos a otorgar al informe[157] especialmente si el experto se basa en testimonios de oídas para sustentar sus conclusiones.[158] En Bemba et al., las capturas de pantalla de Facebook utilizadas por la Fiscalía para vincular a dos individuos fueron impugnadas por la defensa "sobre la base de que la titularidad de la cuenta de Facebook no podía verificarse desde el método forense y que no había metadatos asociados a las capturas de pantalla".[159]

Las buenas prácticas para investigaciones basadas en DOSI ya exigen mantener un rastro detallado sobre la recolección de información y la cadena de custodia.[160] Esto ayuda a garantizar transparencia, accesibilidad y, potencialmente, replicabilidad.[161] Los medios técnicos, tales como herramientas de captura de sitios web,[162] pueden contribuir a automatizar el proceso. Sin embargo, dicho rastro puede ser solo parcial y la replicación no siempre será posible, ya que miles de funciones automatizadas se ejecutan al realizar cualquier búsqueda en línea. Debido a los algoritmos de búsqueda, dos personas que introduzcan los mismos términos pueden obtener resultados distintos. En consecuencia, si bien los expertos deben procurar apegarse a enfoques objetivamente verificables,[163] el método científico tradicional basado en la replicabilidad no encaja del todo en el contexto de la DOSI.

Esta incongruencia reafirma la necesidad de adoptar directrices claras, o al menos alcanzar entendimientos comunes entre la judicatura, las partes y la comunidad DOSI en general, respecto de la admisibilidad y el peso de la prueba pericial basada en DOSI.[164] La dificultad de replicar búsquedas podría superarse con el avance de la tecnología. Pero, mientras tanto, corresponderá a la judicatura

asegurar que los expertos en DOSI sean examinados rigurosamente acerca de sus métodos, reconociendo al mismo tiempo la penumbra algorítmica de incertidumbre e individualidad que acompaña los análisis DOSI.

Identificar el origen y el creador del material DOSI, cuando sea posible, será importante para evaluar su peso y admisibilidad.[165] La evidencia basada en fuentes anónimas se ha convertido en una categoría paria ante la CPI,[166] sosteniendo que los artículos periodísticos de fuentes abiertas solo pueden admitirse si se establecen suficientemente los antecedentes y cualificaciones de los periodistas o de sus fuentes, en cuanto a su objetividad y profesionalismo.[167]

Subyacentes al rechazo de los rumores anónimos están las preocupaciones de que la capacidad de la parte contraria para impugnar la evidencia se vea menoscabada,[168] y de que la información pueda provenir de una fuente engañosa.[169]

Siempre que sea posible, los equipos de DOSI deben triangular los materiales probatorios, a fin de demostrar el valor probatorio de su peritaje.[170] Esto debe incluir comparaciones con materiales de referencia obtenidos lo más cerca posible en el tiempo respecto del elemento analizado, como la apariencia de una persona (o el sonido de su voz),[171] o de un edificio,[172] u otros elementos, dado que pueden cambiar con el tiempo. Se debe reconocer explícitamente cualquier alteración de los materiales examinados, por ejemplo, para mejorar su visibilidad o sus propiedades de audio (reducción de ruido).[173]

Al mismo tiempo, los equipos deben evitar intentar ponerse en el lugar de los jueces para resolver cuestiones últimas.[174] En lo terminológico, debe evitarse el uso de expresiones judiciales como "más allá de toda duda razonable". Como alternativa, el perito en comparación de voz en Al Hassan utilizó expresiones como "apoya firmemente" y "apoya ligeramente" para explicar sus conclusiones.[175]

Los equipos de DOSI también deben ser conscientes del contexto más amplio de posibles protecciones de derechos humanos. La potencial afectación a la privacidad es un asunto crítico.[176] Los expertos deben asegurarse de que las personas representadas hayan consentido la difusión de su imagen o que exista un fin forense legítimo para mostrarla. Medidas como la distorsión de imagen y voz pueden mitigar intromisiones en la privacidad. Si los especialistas en DOSI presentan materiales adicionales obtenidos por ellos mismos para triangular los materiales que están verificando, nuevamente deben tener cuidado de no violar injustificadamente los derechos de privacidad y la dignidad de otros testigos, víctimas y terceros.

En el plano normativo, contar con regulaciones jurídicas o un instrumento vinculante sobre prueba pericial e DOSI con estatus conforme al Artículo 21 del Estatuto de Roma (como enmiendas a las Reglas de Procedimiento y Prueba, al Reglamento de la Corte, o que califiquen como fuentes en virtud del Artículo 21), permitiría el mayor nivel de coherencia de práctica relativa a este tipo de pruebas.[177] La formalización de la práctica en la ley prescriptiva marcaría la maduración de la DOSI como un área reconocida de especialización relevante desde el punto de vista forense. Asimismo, reflejaría la creciente importancia de la DOSI para la resolución de casos de crímenes atroces. En tanto no se adopten tales disposiciones regulatorias, la comunidad DOSI permanecerá sin un punto de anclaje claro al intentar predecir quién puede calificar como experto en este ámbito, quién debería ser llamado como perito de refutación y cómo se evaluará el valor probatorio de los materiales DOSI.[178] En este contexto, los criterios de la siguiente sección se presentan como una guía para ayudar a identificar expertos en DOSI.

# 5. Criterios para la clasificación como perito experto en DOSI

La creciente prevalencia y relevancia forense de la DOSI exige estándares claros, accesibles, objetivamente justificables y no sesgados para su presentación ante tribunales internacionales como la CPI.[179] Es importante que la Corte mantenga un enfoque riguroso para admitir a una persona como experta, especialmente dada la fácil accesibilidad de la DOSI y su potencial de ser malinterpretada o manipulada. Con estos objetivos en mente, a continuación se presenta una lista de factores destinada a ayudar a determinar si una persona posee la habilidad o conocimiento especializado en el ámbito de la DOSI necesarios para rendir prueba pericial. La lista se basa en jurisprudencia relevante y en leyes nacionales, incluidas las de Estados Unidos[180] y el Reino Unido,[181] donde existe un volumen considerable de litigio que aborda evidencia digital.

Si bien los factores están enumerados en el orden en que normalmente serían considerados al determinar la pericia, no se pretende que dicho orden sea inflexible. Asimismo, no existe necesariamente una jerarquía de importancia entre los factores. Sin embargo, algunos factores son particularmente significativos. como el primero que se describe. Tampoco se pretende que todos los factores sean acumulativos. En cambio, constituyen un conjunto de consideraciones que deben evaluarse en su totalidad para orientar la valoración del tribunal (así como de las partes y de la comunidad DOSI en general) respecto de quién puede calificar como experto en DOSI.

## A. Experiencia y competencia demostrables

El primer y más importante criterio para los peritos en DOSI es la experiencia y competencia demostrables en la aplicación de la pericia pertinente. Esto normalmente se demostraría mediante un portafolio (o registro) de proyectos previos o en curso, junto con los resultados u objetivos alcanzados en esos proyectos, que se hayan idealmente presentado ante instituciones de prestigio. La experiencia y la competencia pueden complementar (o potencialmente sustituir) las cualificaciones formales, siempre que sea evidente la alta calidad y coherencia del trabajo.[182] Contar con amplia experiencia en pruebas técnicas puede ser determinante; un factor para reconocer como experto al perito de comparación de voz en Al-Hassan fue precisamente sus 10 años de trabajo en este campo.[183]

## B. Reconocimiento previo como perito experto

El segundo criterio es cualquier reconocimiento previo como perito (ante un órgano judicial internacional o nacional) en un área de experiencia sustancialmente similar. Tal reconocimiento sirve como indicador de la habilidad y/o conocimiento especializado del experto propuesto. Esto es coherente con el enfoque actual del formulario de solicitud para ser incluido en la lista de expertos.[184] No obstante, la parte que propone al experto debe revelar cualquier información que indique que el estatus de tal persona como perito fue cuestionada en procedimientos anteriores, por ejemplo durante un contrainterrogatorio.[185]

## C. Calificaciones académicas y profesionales

El tercer criterio son las calificaciones académicas y profesionales (o cursos formales realizados).[186] Estas indican que la persona ha cumplido estándares establecidos y que ha sido instruída por especialistas con experiencia en cuestiones técnicas y sistémicas. En este aspecto, el formulario de solicitud de la CPI para ser inscrito como experto hace referencia destacada a la educación formal y solicita copia de las certificaciones del postulante emitidas por el organismo regulador o profesional en el que se encuentre

registrado. Sin embargo, la ausencia de organismos profesionales o reguladores generales en el ámbito DOSI (aunque existan algunos en subáreas relacionadas) entra potencialmente en tensión con el sentido de este requisito,[187] lo que ha generado llamados a crear una forma de certificación o acreditación DOSI con reconocimiento estatal, como se analiza en este artículo.

## D. Conocimiento o habilidad demostrable que exceda lo normalmente disponible para el juzgador de hechos

El cuarto criterio consiste en poseer conocimientos o habilidades que puedan demostrarse superiores a las que suele disponer el juzgador.[188] Dada la naturaleza altamente accesible de la DOSI, corresponderá a la parte que proponga al especialista demostrar por qué la prueba pericial excede lo que podría obtener una persona lega bien informada. Existe una amplia gama de capacidades técnicas entre quienes participan en investigaciones DOSI, desde principiantes sin experiencia hasta profesionales de vasta experiencia y alta competencia técnica, como se observa en el trabajo de los expertos en DOSI en el litigio sobre el MH17.[189] Mantener una exigencia estricta respecto de este criterio es importante porque: (i) los jueces mismos deberían poseer u obtener información o conocimientos fácilmente accesibles; (ii) permitir el dictamen pericial de personas sin conocimientos o habilidades superiores a las de la media plantearía la pregunta de por qué a los demás testigos se les impide aportar opiniones; y (iii) el riesgo de interpretaciones erróneas y errores es, en general, mayor si la persona no ha desarrollado un nivel especializado de conocimiento o habilidad, ya que podría no ser consciente de factores contextuales importantes para la interpretación, de posibles fallas metodológicas y de ejemplos previos en los que se han alcanzado conclusiones erróneas dentro del campo de estudio.

## E. Compromiso con los deberes éticos

El quinto criterio consiste en garantizar que los expertos comprendan y respeten sus deberes éticos, incluidos la integridad, la objetividad y la neutralidad.[190] En cuanto al enfoque de experto a sueldo que se ha desarrollado en algunos ámbitos en relación al dictamen pericial, los tribunales han lamentado con frecuencia que: "... el carácter insatisfactorio, y también peligroso, de este tipo de prueba es bien conocido; hoy en día los expertos son a menudo simples defensores pagados o partidarios de quienes los emplean y pagan, tanto como los abogados que llevan el litigio".[191] Idealmente, la persona propuesta como experta debería haber completado formación en ética, asegurando que comprende el impacto de su trabajo en las comunidades de víctimas, así como principios esenciales como No Hacer Daño, el principio de consentimiento informado y los marcos adecuados para interrogar a testigos.[192]

## F. Integración de la revisión por pares en la metodología de trabajo

Finalmente, como sexto factor, la metodología del experto propuesto debería incluir un nivel de revisión por pares.[193] Aunque esto no es tanto una característica personal como un modo de abordar la labor, constituye un indicio importante del compromiso con generar resultados precisos y defendibles. Esto no solo reduciría el riesgo de que se filtren errores de evaluación, sino que también fomentaría un enfoque más científico y la generación de estándares dentro de la comunidad DOSI. Ello podría, a su vez, contribuir al establecimiento de un tipo más amplio de certificación o acreditación formal en este ámbito.

## G. Consideraciones generales

Los factores cuarto, quinto y sexto, en particular, están dirigidos a mitigar los riesgos asociados con lo que Lord Bingham denominó "farsantes, charlatanes o aficionados entusiastas". Si se permite a una parte presentar un perito que carezca del rigor metodológico suficiente, o cuya metodología no pueda ser examinada, se impondrá a la parte contraria la carga injusta de tener que contrarrestar pruebas que no deberían haber sido admitidas. En el caso de los acusados en procesos penales, podrían surgir graves problemas de derechos humanos derivados de la limitación de su capacidad para impugnar las pruebas en su contra, involucrando el artículo 67 del Estatuto de la CPI. Además, los propios expertos podrían enfrentar demandas por negligencia basadas en su declaración,[194] por lo que tienen un incentivo profesional y legal para evitar exceder el ámbito de su pericia y opinar sobre cuestiones en las que no son verdaderamente expertos.

Al ampliar el rango de personas consideradas expertas y al formular criterios a tener en cuenta, la Corte podría enfrentar acusaciones de arbitrariedad y sesgos potenciales. La CPI debe conducir sus procedimientos sin discriminación por motivos prohibidos.[195] Exigir un alto nivel de habilidad técnica, conocimiento o especialización no vulnera ninguno de esos motivos. Sin embargo, restringir a quienes pueden calificar como expertos solo a personas provenientes de ciertas instituciones, como universidades de élite, o con acceso exclusivo a determinadas certificaciones, correría el riesgo de vulnerar estas importantes protecciones y socavar la creciente accesibilidad de los materiales DOSI para diversas poblaciones, incluidas las comunidades que son víctimas de ataques alrededor del mundo.[196]

Los tribunales han sido durante mucho tiempo cautelosos respecto a expertos que podrían verse contaminados por sesgos derivados de las instrucciones o honorarios que reciben de una de las partes en el proceso.[197] El potencial de una conexión personal inapropiada se refleja en los formularios de solicitud de la CPI para ser inscrito como experto (o como organización experta), que preguntan sobre vínculos con cualquier persona que participe en procedimientos ante la Corte o con miembros de su personal.[198] Las Regulaciones de la Oficina del Fiscal de la CPI confirman que ésta debe implementar controles de sesgo, pero no detallan cómo debe lograrse ni brindan orientación sobre la instrucción de expertos para este fin.[199] Esto constituye una deficiencia significativa, ya que los expertos en áreas relevantes para DOSI serán interrogados sobre sesgos, incluidos los sesgos cognitivos.[200]

Es fundamental que la Corte considere cómo abordar los posibles sesgos en relación con DOSI,[201] desde sesgos políticos o sociales conscientes hasta prejuicios inconscientes, e incluso sesgos algorítmicos particularmente difíciles de detectar.[202] Una forma de controlar dichos sesgos consiste en fomentar que las partes instruyan conjuntamente a los peritos, como intentó la Corte en Lubanga, de modo que "el perito único no se vea influido, ni siquiera de forma inconsciente, por la perspectiva de solo una de las partes" y por lo tanto "pueda presentar una visión equilibrada de los problemas".[203] Sin embargo, ese mecanismo de control solo aborda posibles influencias externas provenientes de las partes en litigio. No contrarresta directamente la posibilidad de sesgos internos, particularmente de carácter inconsciente, que puedan afectar la fiabilidad de la prueba.[204]

Para protegerse frente a esos desafíos, la CPI debería asegurarse de que su enfoque para ampliar la definición de experto en DOSI (o para aplicar la definición existente de una manera más amplia) sea (i) formulado de manera transparente y objetiva, y (ii) basado en una interacción continua con la subcomunidad DOSI, de modo que se mantenga el ritmo tanto con el rápido desarrollo tecnológico como con el avance de los usos indebidos de estas tecnologías que manipulan posibles elementos de prueba.[205] La CPI puede valerse del intercambio con la comunidad DOSI respecto a calificaciones y estándares profesionales para refinar e integrar criterios (como los propuestos anteriormente) en su jurisprudencia y, de ese modo, aportar mayor consistencia y objetividad a su abordaje para determinar

el estatus de experto en DOSI, mientras mitiga el riesgo de que los sesgos afecten su criterio. Esto cobra particular importancia en relación con plataformas y medios que incorporan nuevas funciones, como la integración de IA, a fin de garantizar que la Corte cuente con la comprensión sustantiva y el léxico técnico necesarios para realizar las evaluaciones pertinentes y fundamentar adecuadamente sus decisiones sobre la admisibilidad y el valor probatorio de los materiales DOSI.

# 6. Conclusión

Cuando la CPI inició sus operaciones en 2002, la era digital estaba en su infancia. En las dos décadas transcurridas desde entonces, la creciente ubicuidad de los dispositivos de grabación digital y la facilidad para transferir archivos ha generado un aumento exponencial en la disponibilidad de videos, imágenes y otros tipos de DOSI para procedimientos forenses.[206] Mientras que los tribunales *ad hoc* para la ex Yugoslavia y Ruanda fueron esencialmente tribunales internacionales pre-DOSI, los primeros veinte años de operaciones de la CPI pueden considerarse como el amanecer digital en el cual la DOSI se usaba de manera esporádica y en gran medida como accesorio de la evidencia tradicional. Reflejando ese rol colateral e incidental de la DOSI en esa etapa, el enfoque judicial en la CPI ha sido ad hoc, variable y basado principalmente en transponer las Reglas de Procedimiento y Prueba (de carácter general) a este nuevo tipo de prueba. Dos décadas después, la DOSI se está presentando ante la Corte en mayor cantidad y con mayor relevancia forense que nunca. Conflictos y crisis actuales, como los de Libia, Ucrania y Palestina demuestran que la DOSI inevitablemente desempeñará un papel central en las determinaciones judiciales sobre el resultado de los juicios.

A medida que la DOSI se vuelva más frecuente en los procedimientos penales internacionales, también aumentará el riesgo de que sea malinterpretado. D'Alessandra y Sutherland observan que, en un mundo de "posverdad", el lente suele mentir.[207] Para contrarrestar ese riesgo, las partes oponentes impugnarán la presentación de la DOSI ante el tribunal, así como su fiabilidad y su uso por parte de los jueces al dictar sentencia. Los desafíos técnicos suelen requerir evaluación y evidencia de expertos. Sin embargo, el marco de la CPI para la prueba pericial en materia de DOSI es aún rudimentario. Los principales desafíos surgen de la naturaleza de la DOSI como su posición intermedia entre los ámbitos experto y lego, el carácter colaborativo de los equipos que lo evalúan y los aspectos potencialmente engañosos de la DOSI, además de los sesgos que pueden influir en su interpretación.[208]

Los jueces deben mantener una distinción firme respecto de la categoría de expertos y asegurar un estándar elevado para este tipo privilegiado de declaraciones en los procedimientos internacionales.[209] En particular, los jueces deben desarrollar criterios que sean claros, objetivamente justificables, accesibles, libres de sesgos, pero también lo suficientemente flexibles como para adaptarse a nuevas formas relevantes de pericia. Los seis criterios antes propuestos ofrecen una combinación novedosa para reconocer y regular la presentación de pruebas periciales basadas en DOSI. No obstante, la judicatura no debe limitarse a deferir pasivamente a los expertos en DOSI, sino que también debe capacitarse en esta materia.[210] De este modo, puede ampliar su alfabetización tecnológica, en consonancia con las recomendaciones de la Revisión de Expertos Independientes.[211] A su vez, conforme aumente la competencia de los jueces en materiales digitales, podría elevarse proporcionalmente la exigencia para calificar como experto como consecuencia del requisito de que la especialización del experto exceda el conocimiento del tribunal.[212]

Para la comunidad DOSI, la elaboración de un conjunto de principios ayudaría a que su pericia sea reconocida para fines de calificación formal como expertos. Pero para el caso de ciertos especialistas en DOSI, garantizar que sus equipos adopten metodologías claras y defendibles, un enfoque transparente, revisión por pares y procesos de revisión interna, facilitará que sus conclusiones sean aceptadas por los

jueces en litigios penales internacionales.

La DOSI cuestiona la dicotomía entre expertos y testigos de hecho no expertos. En respuesta a ese desafío, la Corte debe asegurar estándares rigurosos de determinación de hechos y evaluación técnica para los expertos, al tiempo que avanza hacia un enfoque basado en la experiencia y las habilidades para determinar el estatus de experto, en lugar de los modelos tradicionales basados principalmente en la reputación y las credenciales formales de instituciones de élite. Por parte de la comunidad DOSI, deben hacerse esfuerzos para adoptar cualificaciones generales, con la debida atención a las habilidades técnicas, a metodologías robustas y transparentes, y a consideraciones éticas. Este desafío es uno prometedor, que anticipa profundos beneficios para la Corte, las partes en litigio y la comunidad epistémica más amplia interesada en el establecimiento de la verdad y la responsabilidad por los crímenes más graves que aquejan al mundo.

## Notas

1. M. Damaška, Evidence Law Adrift (Yale University Press, 1997), p. 151.

2. La DOSI es información digital disponible en internet que "cualquier miembro del público puede obtener mediante solicitud, compra u observación". Y. McDermott, A. Koenig y D. Murray, "Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations", 19 Journal of International Criminal Justice (JICJ) (2021) 85–105, p. 86. Cuando la DOSI se recopila para utilizarse como evidencia, puede denominarse evidencia digital de fuentes abiertas (EDFA). Véanse A.W. Dutelle, An Introduction to Crime Scene Investigation (Jones & Bartlett Learning, 2016); L. Freeman, "Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials", 41 Fordham International Law Journal (2018) 283–335, p. 297 citando A.R. Gonzales, R.B. Schofield y D.W. Hagy, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, Departamento de Justicia de los Estados Unidos, enero de 2007, p. 72; y R.B. da Silva, "Updating the Authentication of Digital Evidence in the International Criminal Court", 22 International Criminal Law Review (2021) 941–964, pp. 941–942.
La DOSI también puede abarcar varias otras tecnologías, incluidas: (i) inteligencia geoespacial y teledetección (GEOINT); (ii) DOSI obtenida en línea; (iii) inteligencia financiera (FININT); y (iv) tecnologías de documentación. Existen otros términos superpuestos para materiales digitales, como inteligencia de fuentes abiertas (OSINT); L. Freeman, "Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court", en S. Dubberley, A. Koenig y D. Murray (eds.), Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability (Oxford University Press, 2020), 48–67, pp. 48–49. También información de fuentes abiertas (OSI) y contenido audiovisual en línea (OAVC); D. Minogue, S. Allen y Y. McDermott, Putting Principles Into Practice: Testing Open-Source Video as Evidence in the Criminal Courts of England and Wales, Lessons Learned From a Mock Voir Dire Hearing, Global Legal Action Network y Bellingcat, 24 de octubre de 2022, disponible en https://policycommons.net/artifacts/2962219/14ee1a_0cff5b64a9684101a21f96f9e8af7c0a/3770345, §§ 2, 5. Véase también D. Minogue et al., "Putting Principles into Practice: Reflections on a Mock Admissibility Hearing on Open Source Evidence", en M.L. Fremuth y K. Stavrou (eds.), International Criminal Law before Domestic Courts (MANZ Verlag Vien, de próxima publicación; en archivo con los autores). Este artículo emplea el término DOSI, ya que cubre una amplia gama de materiales relevantes para los procesos penales internacionales sin limitar la categoría a videos o imágenes ni restringirla únicamente a materiales de inteligencia.

3. La DOSI normalmente requerirá prueba pericial debido a su naturaleza técnica y cada vez más sofisticada; véase infra, Sección 2.

4. Decision on the Prosecutor's Motion Opposing the Testimony of Witness DE4-30 as a Factual Witness, Ndindiliyimana et al. (ICTR-00-56-T), Sala de Primera Instancia II, 16 de mayo de 2007, § 9 ("cuando una parte decide llamar a una persona como testigo fáctico, y no como perito, implícitamente opta por limitar su declaración a asuntos que dicha persona haya visto, oído o experimentado personalmente").

5. Judgment pursuant to Art. 74 of the Statute, Bemba et al. (ICC-01/05-01/13-1989), Sala de Primera Instancia VII, 19 de octubre de 2016, § 20 ("Bemba et al.Trial JudgmentVéase también A. Appazov, Expert Evidence and International Criminal Justice (Springer, 2016), p. 19; K.M. Richmond y A.P. Sebastiano, "Between Fact and Opinion: The Sui Generis Approach to Expert Witness Testimony in International Criminal Trials", 22 ICLR (2021) 1016–1043, p. 1017.

6. R. Wilson, Incitement on Trial: Prosecuting International Speech Crimes (Cambridge University Press, 2017), p. 228. Los

juicios internacionales suelen contar con un número significativo de expertos. Por ejemplo, en el juicio Ongwen ocho peritos prestaron declaración: Trial Judgment, Ongwen (ICC-02/04-01/15), Sala de Primera Instancia IX, 4 de febrero de 2021, §§ 594–602.

7. Véase infra Sección 4.

8. Appazov, supra nota 5, pp. 5–7.

9. Véase, por ejemplo, A. Koenig et al., "Open Source Fact-Finding in Preliminary Examinations", en M. Bergsmo y C. Stahn (eds.), Quality Control in Preliminary Examinations, vol. 2 (Torkel Opsahl Academic EPublisher, 2018), pp. 681–710; Freeman (2020), supra nota 2, p. 48.

10. Véase, por ejemplo, F. D'Alessandra y K. Sutherland, "The Promise and Challenges of New Actors and New Technologies in International Justice", 19 JICJ (2021) 9–34, que se centra en la información digital y su uso para investigaciones por mecanismos de rendición de cuentas, y contiene referencias superficiales a conclusiones periciales en casos existentes o ya cerrados, pero no analiza en absoluto el rol de los expertos en litigio; Minogue, Allen y McDermott, supra nota 2, que aborda la prueba pericial y la IDFADOSI, pero únicamente en el contexto de procesos internos bajo el derecho del Reino Unido; E. McPherson et al., "Open Source Investigations and the Technology-driven Knowledge Controversy in Human Rights Fact-finding", en Dubberley, Koenig y Murray (eds.), supra nota 2, pp. 68–86, que se enfoca en expertos en determinación de hechos en derechos humanos sin abordar el Estatuto de Roma, las Reglas de Procedimiento y Prueba, ni otros procedimientos legales conforme a los cuales dichas conclusiones serían admitidas como prueba y utilizadas ante tribunales internacionales o nacionales; A. Koenig y L. Freeman, "Open Source Investigations for Legal Accountability: Challenges and Best Practices", en Dubberley, Koenig y Murray, supra nota 2, pp. 331–342, pp. 340–341, que hace referencias superficiales al dictamen pericial sobre DOSI sin abordar el Estatuto de la CPI ni las Reglas de Procedimiento ni otras normas jurídicas internacionales.

11. Véase, por ejemplo, Office of the United Nations High Commissioner for Human Rights and University of California Berkeley School of Law, Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law (en adelante, el "Berkeley Protocol"), 3 de enero de 2022, § 213 (menciona a los expertos sin profundizar en las reglas, principios, jurisprudencia y prácticas pertinentes); Interpol, Global Guidelines for Digital Forensics Laboratories, mayo de 2019 (contiene una breve sección sobre peritos, de menos de media página, sin referencias a literatura, jurisprudencia o disposiciones legales); y J. Drake y T. Harris, Geospatial Evidence in International Human Rights Litigation: Technical and Legal Considerations, American Association for the Advancement of Science (2018), disponible en línea en https://www.aaas.org/resources/geospatial-evidence-international-human-rights-litigation-technical-and-legal (que aborda el estándar para presentar prueba pericial, pero se enfoca exclusivamente en tecnologías geoespaciales, en lugar de la DOSI de manera más amplia).

12. Véase infra Sección 5.

13. R. Vecellio Segate, "Cognitive Bias, Privacy Rights, and Digital Evidence in International Criminal Proceedings: Demystifying the Double-Edged AI Revolution", 21 ICLR (2021) 242–279, p. 266.

14. K. Hellwig, "The Potential and the Challenges of Digital Evidence in International Criminal Proceedings", 22 ICLR (2021) 965–988, p. 982.

15. J. Hendrix, "Ukraine May Mark a Turning Point in Documenting War Crimes", Just Security", 28 de marzo de 2022, disponible en https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/; C. Quilling, "The Future of Digital Evidence Authentication at the International Criminal Court", Journal of Public and International Affairs, 20 de mayo de 2022, disponible en https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court.

16. K. MacLean, "Interactive Digital Platforms, Human Rights Fact Production, and the International Criminal Court", 15 Journal of Human Rights Practice (JHRP) (2023) 84–99, pp. 85–88.

17. Véase, por ejemplo, L. Ten Hulsen, "Open Sourcing Evidence from the Internet – The Protection of Privacy in Civilian Criminal Investigations Using OSINT (Open-Source Intelligence)", 12 Amsterdam Law Forum (2020) 1–45, para una discusión sobre consideraciones de privacidad en el uso de OSINT en investigaciones penales.

18. D'Alessandra y Sutherland, supra nota 10.

19. Detailed Findings of the Independent International Fact-finding Mission on the Bolivarian Republic of Venezuela, Doc. ONU A/HRC/45/CRP.11, 15 de septiembre de 2020.

20. Véase, por ejemplo, M. Browne, D. Botti and H. Willis, "Satellite Images Show Bodies Lay in Bucha For Weeks, Despite Russian Claims", New York Times, 4 de abril de 2022, disponible en https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html; Y. Al-hlou et al., "Caught on Camera, Traced by Phone: The Russian Military Unit that Killed Dozens in Bucha", New York Times, 22 de diciembre de 2022, disponible en https://www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html.

21. Véase, por ejemplo, District Court of The Hague, "Transcript of the MH17 Judgment Hearing", 17 de noviembre de 2022,

disponible en https://www.courtmh17.com/en/news/2022/transcript-of-the-mh17-judgment-hearing.html (observando el rol de las fotos y videos de fuente abierta). Véase también Bellingcat, "A Post Mortem of Russia's Claim that Crucial MH17 Video Evidence was Falsified", 10 de marzo de 2020, disponible en https://www.bellingcat.com/news/2020/03/10/a-post-mortem-of-russias-claim-that-crucial-mh17-video-evidence-was-falsified/; Freeman, supra nota 2.

22. Aunque la prueba pericial es particularmente relevante para la admisión y valoración de DOSI en la CPI, los análisis expuestos en este artículo también son pertinentes para otros tribunales internacionales penales y civiles que puedan encontrarse con DOSI, como las Salas Especializadas para Kosovo; el Mecanismo para los Tribunales Penales Internacionales; y las Cámaras Extraordinarias de los Tribunales de Camboya; así como tribunales nacionales que actúan bajo jurisdicción universal.

23. L. Freeman y R. Vázquez Llorente, "Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age", 19 JICJ (2021) 163–188, p. 168.

24. La verificación digital es un proceso que utiliza técnicas como la geolocalización ("la identificación o estimación del lugar donde se encuentra un objeto, una actividad o el lugar desde el cual se generó un elemento") y la cronolocalización ("la corroboración de las fechas y horas de los eventos representados en una pieza de información"); Berkeley Protocol, p. 65, así como búsquedas inversas de imágenes para verificar la ubicación, fecha y autenticidad del material digital; A. Toler, "How To Verify and Authenticate User Generated Content", en Dubberley, Koenig y Murray (eds), supra nota 2, 185–227. Puede hacerse una distinción entre verificación digital y forensia digital, siendo esta última un examen y análisis en el que "los métodos van desde pruebas técnicas y computacionales que analizan los archivos [digitales] en sí mismos para detectar anomalías o repeticiones no naturales, hasta la inspección visual del contenido representado en el archivo, incluida la separación de cuadros en imágenes fijas y la búsqueda de los llamados 'artefactos de manipulación'"; Minogue, Allen y McDermott, supra nota 2, §§ 87, 91–92; Hellwig, supra nota 14, p. 982. Sin embargo, el presente análisis adopta una perspectiva global de la pericia en DOSI debido a que las reglas de procedimiento y evidencia de la CPI, especialmente aquellas relativas los expertos, son de naturaleza generalista, enfocándose en la forma de la evidencia (declaración de testigos, documento u otra) en lugar del subcampo específico de la pericia relevante a la evidencia.

25. K.M. Moriarty, "Why are Authentication and Authorization so Difficult?", Center for Internet Security, 18 de octubre de 2021; Hellwig, supra nota 14, p. 982; McDermott, Koenig y Murray, supra nota 2, p. 86. En este sentido, el perito en autenticación de voz en Al-Hassan fue contrainterrogado acerca de si cumplía con su propio procedimiento interno estándar y reconoció que tuvo que modificar los procedimientos, ya que en ese momento estaban cambiando el protocolo pertinente; Transcripción del juicio del 15 de octubre contra Al Hassan, infra nota 106, pp. 27–28, 41.

26. S. Trevisan, "Open-Source Information in Criminal Proceedings: Lessons from the International Criminal Court and the Berkeley Protocol", 4 Giurisprudenza Penale Web (2021) 1–17, p. 1; Freeman (2020), supra nota 2, p. 51.

27. Vecellio Segate, supra nota 13, p. 249, citando A. Duffy, "Bearing Witness to Atrocity Crimes: Photography and International Law", 40 Human Rights Quarterly (2018) 776–814, pp. 803–812.

28. El caso Al-Mahdi es una excepción, y aun en ese caso, su condena se basó principalmente en su declaración de culpabilidad y confesión correspondiente: S. Zarmsky, "Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law", 19 JICJ (2021) 213–225, p. 215.
No obstante, la DOSI se utiliza cada vez más de manera accesoriadurante la etapa probatoria. Por ejemplo, en el caso Ntaganda, la amistad en Facebook entre un testigo y otro fue utilizada para poner en duda la credibilidad del testigo: Sentencia, Ntaganda (ICC-01/04-02/06-2359), Sala de Primera Instancia VI, 8 de julio de 2019, § 226, n. 553.

29. D'Alessandra y Sutherland, supra nota 10; McDermott, Koenig y Murray, supra nota 2, p. 86; Trevisan, supra nota 26, p. 13.

30. Véase la opinión disidente de la Jueza Anita Usacka, Judgment on the appeal of Mr Thomas Lubanga Dyilo against his conviction, Lubanga (ICC-01/04-01/06-3121-Anx2), Sala de Apelaciones, 1 de diciembre de 2014, en la que lamenta que los videos no estén disponibles para su visualización por el público.

31. Véase Judgment pursuant to Art. 74 of the Statute, Lubanga (ICC-01/04-01/06-2842), Sala de Primera Instancia I, 14 de marzo de 2012 ("Bemba et al. Trial Judgment"), § 869 (sin embargo, estos videos fueron introducidos mediante el testigo P-0030, quien no era perito); y Judgment on the appeal of Mr Thomas Lubanga Dyilo against his conviction, Lubanga (ICC-01/04-01/06-3121), Sala de Apelaciones, 1 de diciembre de 2014 ("Lubanga Appeal Judgment"), §§ 200, 223.

32. Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Art. 64(9) of the Rome Statute, Bemba (ICC-01/05-01/08-2299), Sala de Primera Instancia III, 8 de octubre de 2012 ("Bemba Admissibility Decision"), § 120. Esta prueba no constituía estrictamente DOSI en el sentido actual, pero se planteaban consideraciones análogas.

33. Judgment on the appeal of Mr Jean-Pierre Bemba Gombo against Trial Chamber III's Judgment pursuant to Art. 74 of the Statute, Bemba (ICC-01/05-01/08-3636), Sala de Apelaciones, 8 de junio de 2018 ("Bemba Appeal Judgment"), § 183. Compárese

con la Bemba Admissibility Decision, ibid., §§ 9, 123, 128, y con el Bemba Appeal Judgment, ibid., § 183, fns. 366–367, que remiten a la nota 1304 de la sentencia de primera instancia, donde se hace referencia a los mismos videoclips (CAR-OTP-0031-0099, CAR-OTP-0031-0099, CAR-OTP-0031-0093, CAR-OTP-0031-0120, CAR-OTP-0031-0124).

34. Trevisan, supra nota 26, pp. 2 y 12, citando el Bemba et al. Trial Judgment., supra nota 5.

35. Agreement regarding admission of guilt, Al Mahdi (ICC-01/12-01/15-78-Anx1-tENG-Red), Office of the Prosecutor & Defence, 25 de febrero de 2016, Anexo 1, § 14.

36. Véase Forensic Video Analysis Report HAK, Al Hassan (MLI-OTP-0069-9281), Oficina de la Fiscalía, 31 de marzo de 2020 ("Amy Hak Forensics Report"), pp. 80–81. En este caso declararon varios otros peritos, parte de cuya prueba se refirió a cuestiones de DOSI. Véase también Trevisan, supra nota 26, pp. 10–11.

37. Véase M. Perelman, "ICC Chief Prosecutor Sends Warning to Libyan Strongman Haftar", France 24, 16 de diciembre de 2019, disponible en https://www.france24.com/en/africa/20191216exclusive-interview-icc-chief-prosecutor-sends-warning-libyan-strongman-haftar-ivory-coast-palestine-afghanistan-myanmar-philippines.

38. Véase Warrant of Arrest, Al-Werfalli (ICC-01/11-01/17), 15 de agosto de 2017, §§ 11–22; Second Warrant of Arrest, Al-Werfalli (ICC-01/11-01/17), 4 de julio de 2018, §§ 17–18; J. Dettmer, "Video Emerges of IS-style Mass Killing of Jihadists in Libya", Voice of America, 24 de julio de 2017, disponible en https://www.voanews.com/a/video-islamic-state-style-mass-killing-jihadists-libya/3957079.html.

39. "Footage surfaces showing Libya's Haftar 'ordering war crimes'", The New Arab, 20 de septiembre de 2017, disponible en https://www.newarab.com/news/footage-surfaces-showing-libyashaftar-ordering-war-crimes.

40. Véase, p. ej., Al-hlou et al., supra nota 20.

41. Véase, p. ej., Report of the Independent International Commission of Inquiry on Ukraine, A/78/540, 19 de octubre de 2023, § 12.

42. Véase, p. ej., G. Jones, "Russian TV Presenter Says Sorry but Faces Probe for Call to Drown Ukrainian Children", 24 de octubre de 2022, disponible en https://www.reuters.com/world/europe/russian-tv-presenter-says-sorry-faces-probe-call-drown-ukrainian-children-2022-10-24/.

43. Véase, p. ej., S. Zarmsky y J. Mionki, "Symposium on Fairness, Equality, and Diversity in Open Source Investigations", Opinio Juris, 10 de febrero de 2023, disponible en https://opiniojuris.org/2023/02/10/symposium-on-fairness-equality-and-diversity-in-open-source-investigationsout-in-the-open-fair-trial-rights-and-open-source-evidence-at-the-icc/.

44. Véase la Sección 5 infra.

45. La adopción de enmiendas a las Reglas de Procedimiento y Prueba requiere una mayoría de dos tercios de los Estados Partes (art. 51(2)). Los jueces también pueden adoptar disposiciones con carácter provisional por una mayoría de dos tercios (art. 51(3)); véase K. Sharma, "The Curious Case of Rule 165 of the Rules of Procedure and Evidence: The Effect of Control Exercised by the Assembly of States Parties over the International Criminal Court", 20 ICLR (2020) 285. Los jueces pueden modificar el Reglamento de la Corte por mayoría absoluta y también pueden enmendar el Chambers Practice Manual (actualmente, 6.ª ed., 2022), aunque el Manual es solo orientativo y no vinculante.

46. Véase Minogue, Allen y McDermott, supra nota 2, § 90; Freeman (2020), supra nota 2, p. 65.

47. B. Allyn, "Deepfake Video of Zelensky could be 'tip of the iceberg' in Info War, Experts Warn", National Public Radio, 16 de marzo de 2022, disponible en línea en https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia?t=1660657155956.

48. D'Alessandra y Sutherland, supra nota 10, p. 24.

49. Véase, por ejemplo, Zarmsky, supra nota 28, p. 214. Ello no significa que la evidencia de reconstrucción digital sea intrínsecamente inadmisible. Véase también Vecellio Segate, supra nota 13, p. 255 (sobre el carácter seductor de la evidencia en video).

50. Ya existe una creciente demanda de personal con competencias en verificación de videos e imágenes en los mecanismos de rendición de cuentas en Ginebra; véase D. Murray, Y. McDermott y A. Koenig, "Mapping the Use of Open-Source Research in UN Human Rights Investigations", 14 JHRP (2022) 554–581.

51. D'Alessandra y Sutherland, supra nota 10, p. 24.

52. Véase infra, Sección 4, para un análisis de los expertos en verificación de audio y video en Al Hassan. Existen otras vías para la admisión de DOSI, incluida la autenticación mediante el testimonio de testigos con conocimiento personal de que la prueba es lo que pretende ser; P.W. Grimm, D.J. Capra y G.P. Joseph, "Authenticating Digital Evidence", 69 Baylor Law Review (2017) 1–55.

53. Vecellio Segate, supra nota 13, p. 243.

54. R. Gallmetzer, "The Trial Chamber's Discretionary Power to Devise the Proceedings Before it and its Exercise in the Trial of Thomas Lubanga Dyilo", en C. Stahn y G. Sluiter (eds.), The Emerging Practice of the International Criminal Court (Brill, 2009)

501–524, p. 507; MacLean, supra nota 16, p. 85; Freeman, supra nota 2, p. 50; Appazov, supra nota 5, p. 3. Véase también Corrigendum to Decision on the admissibility of four documents, Lubanga (ICC-01/04-01/06-1399-Corr), Sala de Primera Instancia I, 21 de enero de 2011, § 26.

55. Véase infra Sección 5 (sobre enfoques nacionales respecto de la prueba pericial).

56. Véase A. Singh, "Expert Evidence", en K.A.A. Khan, C. Buisman y C. Gosnell (eds.), Principles of Evidence in International Criminal Justice (Oxford University Press, 2010) 599–649, p. 611, citando Oral Decision on Qualification of Prosecution Expert Sebahire Deo Mbonyikebe, Bizimungu et al. (ICTR-99-50-T), Sala de Primera Instancia II, 2 de mayo de 2005 ("Bizimungu Expert Qualification Decision"); Appeals Judgment, Simba (ICTR-01-76-A), Sala de Apelaciones, 27 de noviembre de 2007, § 174; Oral Decision on the Qualification of Mr Edmond Babin as Defence Expert Witness, Ndayambaje et al. (ICTR-98-42-T), Sala de Primera Instancia II, 13 de abril de 2005, § 5.

57. Decision on Defence Preliminary Challenges to Prosecution's Expert Witnesses, Ntaganda (ICC-01/04-02/06-1159), Sala de Primera Instancia VI, 9 de febrero de 2016, § 7, citando inter alia la "Decision on Joint Defence Interlocutory Appeal concerning the Status of Richard Butler as an Expert Witness", Popović et al. (IT-05-88-AR73.2), Sala de Apelaciones, 30 de enero de 2008 ("Popović Butler Appeal Decision"), § 27.

58. Singh, supra nota 56, pp. 614–615.

59. Véase CPI, "Experts", disponible en línea en https://www.icc-cpi.int/get-involved/experts.

60. Véase infra Sección 2.

61. Véase CPI, "Experts", supra nota 59.

62. Sentencia de primera instancia, Bemba et al., supra nota 5, § 20. D. Dwyer, "The Judicial Assessment of Expert Evidence" (Cambridge University Press, 2008), p. 78; Richmond y Sebastiano, supra nota 5, p. 1017.

63. Véase, por ejemplo, Transcripción, Bemba et al. (ICC-01/05-01/13-T-11-Red-ENG), Sala de Primera Instancia VII, 30 de septiembre de 2015, p. 6. Véase también Appazov, supra nota 5, p. 19 (los peritos pueden explicar "por qué determinados hechos permiten inferencias determinadas").

64. Appeal Judgment, Semanza (ICTR-97-20-A), Sala de Apelaciones, 20 de mayo de 2005 ("Semanza Appeal Judgment"), § 303.

65. Dwyer, supra nota 62, p. 2; y C.M. Milroy, "A Brief History of the Expert Witness", 7 Academic Forensic Pathology (2017) 516–526.

66. Decision on Defence Preliminary Challenges to Prosecution's Expert Witnesses, Ntaganda (ICC-01/04-02/06-1159), Sala de Primera Instancia VI, 9 de febrero de 2016, § 9. Véase también Trial Judgement, Ongwen (ICC-02/04-01/15), Sala de Primera Instancia IX, 4 de febrero de 2021, § 2531.

67. Singh, supra nota 56, pp. 615–616.

68. Véase por ejemplo Decision on Prosecution Request to Exclude Defence Witness D-22-0004, Bemba et al. (ICC-01/05-01/13-1653), Sala de primera instancia VII, 24 de febrero de 2016 ("Bemba et al. Witness Exclusion Decision"), § 18; Decision on Prosecution Motion for Reconsideration of the Decision on Prospective Experts Guichaoua, Nowrojee and Des Forges, or for Certification, Karemera et al. (ICTR-98-44-T), Sala de primera instancia III, 16 de noviembre de 2007, § 21; Decision on Report of Prosecution Expert Klaus Reinhardt, Hadžihasanov and Kubura (IT-01–47-T), Sala de primera instancia II, 11 de febrero de 2004, p. 4. Véase también M. Gillett, Prosecuting Environmental Harm before the International Criminal Court (Cambridge University Press, 2022), pp. 197–198; Singh, supra nota 56, p. 601.

69. Decision on Sang Defence Application to exclude Expert Report of Mr Hervé Maupeu, Ruto and Sang (ICC-01/09-01/11-844), Sala de Primera Instancia V(a), 7 de agosto de 2013, § 13..

70 Singh, supra note 56, p. 618, citando la Order Relating to Defence Witness Bernard Lugan, Karemera et al. (ICTR-98-44-T), Sala de Primera Instancia III, 5 de mayo de 2008, § 7.

71. Por ejemplo, en Nahimana, que versaba sobre la responsabilidad de los dirigentes de una emisora de radio privada ruandesa por incitación al genocidio, el TPIR aceptó prueba pericial indicando que había "ataques generalizados contra la población tutsi en todo Ruanda" y que "RTLM [la emisora] tuvo un enorme impacto en la situación, alentando los asesinatos de tutsis y de quienes los protegían". Singh, supra note 56, p. 618, citando la Decision on the Expert Witnesses for the Defence, Nahimana et al. (ICTR-99-52-A), Sala de Primera Instancia I, 24 de enero de 2003, y la Trial Judgment, Nahimana et al. (ICTR-99-52-T), Sala de Primera Instancia I, 3 de diciembre de 2003, § 458.

72. Bemba et al. Witness Exclusion Decision, supra note 68, § 11..

73. Lubanga Trial Judgment, supra note 31, § 11 (sin embargo, la Fiscalía no presentó prueba pericial respecto del asunto crítico del juicio, la edad de los niños que aparecían en videos en el entorno de Lubanga; véase Lubanga Appeals Judgment, §§ 187–188);Judgment

pursuant to Art. 74 of the Statute, Katanga (ICC-01/04-01/07-3436-tENG), Sala de Primera Instancia II, 7 de marzo de 2014, § 21.

74 Reglamento 44(2) del Reglamento de la Corte de la CPI.

75. L. Baddour, "International Criminal Law and Common Law Rules of Evidence", en Khan, Buisman y Gosnell (eds), supra nota 56, 96, pp. 110–111. Escuchar a múltiples peritos de manera simultánea se ha denominado coloquialmente "hot-tubbing"; Decision on Simultaneous or Concurrent Testimony of Expert Witnesses, Ayyash et al. (STL-11-01/T/TC), Sala de Primera Instancia, 17 de febrero de 2015, §§ 12–39.

76. Singh, supra nota 56, p. 606.

77. Véase Singh, supra nota 56, pp. 599, 606.

78. Decision on the Prosecutor's Bar Table Motions, Katanga and Ndudjolo (ICC-01/04-01/07), Sala de Primera Instancia II, 17 de diciembre de 2010 ("Katanga and Ngudjolo Bar Table Motions"), § 24(a) y (d).

79. Véase Trevisan, supra nota 26, p. 4.

80. Véase N. Mehandru y A. Koenig, "ICTs, Social Media, & the Future of Human Rights", 17 Duke Law and Technology Review (2019) 129–145, p. 135.

81. Véase también Bemba et al. Sentencia de juicio, supra nota 5, § 247.

82. Decision adjourning the hearing on the confirmation of charges pursuant to Art. 61(7)(c)(i) of the Rome Statute, Gbagbo (ICC-02/11-01/11-432), Sala de Cuestiones Preliminares I, 3 de junio de 2013 ("Gbagbo Confirmation Adjournment"), §§ 28–35.

83. Freeman (2020), supra nota 2, p. 50, citando Decision on the admission into evidence of items deferred in the Chamber's "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute", Bemba (ICC-01/05-01/08-2721), Sala de Primera Instancia III, 27 de junio de 2013.

84. Véase D. Sorvatzioti, "Free Evaluation of Evidence: Does the ICC need a Law of Evidence?", 22 ICLR (2021) 895–919, p. 905.

85. Véase R. Glover, Murphy sobre Evidence (15.ª ed., Oxford University Press, 2017), sección 2.5.1.

86. Decision on the Admission into Evidence of Intercept Related Materials, Blagojevic and Jokic (IT-02-60-T), Sala de Primera Instancia I, 18 de diciembre de 2003, § 25; Decision Adopting Guidelines on the Standards Governing the Admission of Evidence, Martic (IT-95-11-T), Sala de Primera Instancia I, 19 de enero de 2006, § 7.

87. Véase supra nota 45 sobre las opciones de enmienda de los distintos instrumentos de la Corte. Entre los actores de la sociedad civil, diversas organizaciones han elaborado directrices —como el Berkeley Protocol y el actual proyecto de la Nuremberg Principles Academy sobre prueba digital—, pero ninguna ha sido adoptada oficialmente por la CPI como fuentes de derecho del tipo previsto en el art. 21. Véase también Vecellio Segate, supra nota 13, p. 249.

88. Véase, por ejemplo, Hellwig, supra nota 14, nota al pie 131; Freeman (2020), supra nota 2, p. 64; Vecellio Segate, supra nota 13, p. 249. La prueba documental es información registrada en cualquier soporte que se presenta para acreditar un hecho en función de esa información (típicamente para demostrar la veracidad de su contenido); Glover, supra nota 85, sección 2.5.1; M. Nerenberg y W. Timmermann, "Documentary Evidence", en Khan, Buisman y Gosnell (eds), supra nota 56, pp. 443–498.

89. Por ejemplo, S. Aalto-Setälä et al., supra nota 78, sección A5, citando Katanga and Ngudjolo Bar Table Motions, supra nota 78, § 24 (señalando que un video será admitido como prueba "material"). La prueba material consiste en objetos tangibles que pueden presentarse ante el tribunal (según las limitaciones logísticas) para mostrar su estado y a partir de los cuales "el tribunal de hecho puede extraer conclusiones basadas en su propia percepción"; Glover, supra nota 86, sección 2.5.1.

90. En la audiencia simulada de voir dire realizada por Global Legal Action Network (GLAN), Bellingcat y el proyecto OSR4Rights de la Universidad de Swansea, el material de video DOSI (denominado OAVC en ese ejercicio) fue descrito de varias maneras, incluyendo: prueba material; prueba documental; y prueba documental que contiene prueba material; Minogue, Allen y McDermott, supra nota 2, §§ 49, 57.

91. En relación con la prueba pericial como prueba testimonial, véase Decision on the Prosecution's Applications for Introduction of Prior Recorded Testimony under Rule 68(2)(b) of the Rules, Ongwen (ICC-02/04-01/15-596-Red), Sala de Primera Instancia IX, 18 de noviembre de 2016, § 9 (sosteniendo que una Sala puede permitir la introducción de informes periciales mediante la regla 68 —como la regla 68(3)).

92. Vecellio Segate, supra nota 13, pp. 255–256.

93. Véase, por ejemplo, R v. Lydon (1987) 85 Cr App R 221 (donde se encontró un arma y dos pedazos de papel que decían "Sean rules" ("Sean manda") en la cuneta por la que había pasado un automóvil que la fiscalía buscaba vincular con el acusado, Sean Lydon; se consideró que eran prueba admisible para corroborar una identificación controvertida que conectaba al acusado con el automóvil y, por ende, con un robo, más que para probar que Sean, de hecho, "manda").

94. Katanga and Ngudjolo Bar Table Motions, supra nota 78, § 24(a) y (d).

95. Minogue, Allen y McDermott, supra nota 2, § 67.

96. Por ejemplo, en un caso ante el TEDH, un especialista en DOSI de la organización Bellingcat tuvo que explicar por qué existían en línea dos versiones visualmente contradictorias de una misma imagen, algo que una persona lega no sabría. Véase E. Higgins, "How Open Source Evidence was Upheld in a Human Rights Court", Bellingcat, 28 de marzo de 2023, disponible en https://www.bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court/ refiriéndose a Ukraine and The Netherlands v. Russia, TEDH (solicitudes núm. 8019/16, 43800/14 y 28525/20).

97. Singh, supra nota 56, pp. 623–624. Véase también Richmond y Sebastiano, supra nota 5, p. 1017.

98. D'Alessandra y Sutherland, supra nota 10; W.H. Wiley, "International(ised) Criminal Justice at a Crossroads: The Role of Civil Society in the Investigation of Core International Crimes and the CIJA Model", en Bergsmo y Stahn (eds), supra nota 9, pp. 547–587, en 547.

99. Véase Minogue, Allen y McDermott, supra nota 2, § 76.

100. Bingham LJ en R v. Robb [1991] 93 Cr App R 161, § 166. Véase también la decisión de la jueza Korner según se resume en Minogue, Allen y McDermott, supra nota 2, §§ 76–77.

101. Véase Minogue, Allen y McDermott, supra nota 2, § 67.

102. M. Roache, "Bellingcat Has Revealed War Crimes in Syria and Unmasked Russian Assassins. Founder Eliot Higgins Says They're Just Getting Started", TIME, 2 de marzo de 2021, disponible en línea en https://time.com/5943393/bellingcat-eliot-higgins-interview.

103. Véase, por ejemplo, S. Dubberley, "The Digital Verification Corps: Amnesty International's Volunteers for the Age of Social Media", Amnesty International Citizen Evidence Lab, 6 de diciembre de 2019, disponible en línea en https://citizenevidence.org/2019/12/06/the-digital-verification-corps-amnesty-internationals-volunteers-for-the-age-of-social-media/.

104. Véase Semanza Appeal Judgment, supra nota 64, § 303; Decision on the Motion by the Prosecution to Allow the Investigators to Follow the Trial during the Testimonies of the Witnesses, Delalić et al. (IT-96-21-T), Sala de Primera Instancia, 20 de marzo de 1997, § 10.

105. Véase infra nota 130 para un ejemplo relevante relacionado con Bellingcat.

106. Véase Transcripción, Al Hassan (ICC-01/12-01/18-T-036-Red-ENG), Sala de Primera Instancia X, 15 de octubre de 2020 ("Transcripción del Juicio Al Hassan del 15 de octubre"), p. 6. Debido a las redacciones y a las restricciones sobre la información disponible, no está claro si los elementos examinados eran DOSI o si fueron obtenidos de fuentes no abiertas.

107. Véase, por ejemplo, Joint Prosecution and Defence Submission of the Expert Report, Abd-Al-Rahman (ICC-02/05-01/20-582), 4 de febrero de 2022, § 9.

108. Transcripción del Juicio Al Hassan del 15 de octubre, supra nota 106, pp. 25, 65.

109. Transcripción del Juicio Al Hassan del 15 de octubre, supra nota 106, p. 9.

110. Adjuntó su currículum vitae a su informe pericial; véase Amy Hak Forensics Report, supra nota 36.

111. Amy Hak Forensics Report, supra nota 36, pp. 67–75.

112. Véase CPI, "Application Form: Natural Persons", disponible en línea en https://www.icc-cpi.int/sites/default/files/ICC_Experts_Form_Eng.docx, p. 5.

113. MacLean, supra nota 16, pp. 85–88; N. Hughes, U. Karabiyik, "Towards Reliable Digital Forensics Investigations Through Measurement Science", 2 WIRES Forensic Science (2020) 1367–1377, p. 1367.

114. Véase, por ejemplo, Human Rights Center, UC Berkeley School of Law y el Institute of International Criminal Investigations, "Course: Open Source Investigation–Foundational", disponible en línea en https://iici.global/course/open-source-investigation-foundational; Bellingcat, "Workshops", disponible en línea en https://www.bellingcat.com/workshops; Amnistía Internacional, "Open source investigations for human rights: Part 1", Advocacy Assembly, disponible en línea en https://advocacyassembly.org/en/courses/57; Atlantic Council, "360/Digital Sherlocks", disponible en línea en https://www.digitalsherlocks.org.

115. Véase, por ejemplo, Centre of Governance & Human Rights, "Open Source Investigation for Academics", University of Cambridge, disponible en línea en https://www.cghr.polis.cam.ac.uk/projects/open-source-investigation-academics; UCLA School of Law, "Human Rights and War Crimes Digital Investigations", disponible en línea en https://law.ucla.edu/academics/curriculum/human-rights-and-war-crimes-digital-investigations.

116. Véase, por ejemplo, IntelTechniques, "Video Training + Certification", disponible en línea en https://www.inteltechniques.net/bundles/video-training-certification; Global Information Assurance Certification, "GIAC Open Source Intelligence Certification (GOSI)", disponible en línea en https://www.giac.org/certifications/open-source-intelligence-gosi.

117. Minogue, Allen y McDermott, supra nota 2, § 76.

118. Singh, supra nota 56, p. 614.

119. Íbid., citando la Bizimungu Expert Qualification Decision, supra nota 56.

120. Singh, supra nota 56, pp. 614–615, citando la Public Transcript of Hearing, Bizimungu et al. (ICTR-99-50-T), Sala de Primera Instancia II, 25 de abril de 2006, pp. 3–4.

121. Singh, supra nota 56, p. 615, refiriéndose a la calificación que hizo la Sala de Primera Instancia del TPIR en Nahimana et al. de un perito de la fiscalía, Kabanda, en materia de prensa escrita, sobre la base de que "de una lista de 51 publicaciones, revistas y diarios que se le presentaron, él conocía o estaba familiarizado con 43 de ellas". Véase también Decision on Expert Witness PRH348, Mr Geyer, Ayyash et al. (STL-11-01/T/TC), Sala de Primera Instancia, 16 de julio de 2014.

122. Art. 21(3) del Estatuto de Roma.

123. Véase infra, Sección 5.

124. Véase, por ejemplo, los casos del TPIY mencionados anteriormente, en los cuales la mayoría de los peritos admitidos prepararon sus informes individualmente; infra, Sección 3.

125. Pero una Sala de Primera Instancia "puede solicitar la asistencia de peritos y otros organismos": Judgment on the appeals against the order of Trial Chamber II of 24 March 2017 entitled "Order for Reparations pursuant to Article 75 of the Statute", Katanga (ICC-01/04-01/07-3778-Red), Sala de Apelaciones, 9 de marzo de 2018, § 72.

126. Decision on the Procedures to be Adopted for Instructing Expert Witnesses, Lubanga (ICC-01/04-01/06-1069), Sala de Primera Instancia I, 10 de diciembre de 2007, § 14.

127. Véase CPI, "Application Form: Expert Organizations", disponible en línea en https://www.icc-cpi.int/sites/default/files/ICCExpertsForm0_English.docx, p. 3.

128. A. Koenig, "Open Source Evidence and Human Rights Cases: A Modern Social History", en Dubberley, Koenig y Murray (eds), supra nota 2, 32–47, en 39–40.

129. Véase D'Alessandra y Sutherland, supra nota 10.

130. Véase la cooperación entre Bellingcat y Forensic Architecture, Bellingcat Investigation Team, "We are going to surrender! Stop shooting!": Reconstructing Oscar Pérez's Last Hours", Bellingcat, 13 de mayo de 2018, disponible en línea en https://www.bellingcat.com/news/americas/2018/05/13/we-are-going-to-surrender-stop-shooting-reconstructing-oscar-perezs-last-hours/.

131. A. Koenig y L. Freeman, "Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation", 73 Hastings Law Journal (2022) 1233–1254, en 1235.

132. Europol, "Stop Child Abuse—Trace an Object", disponible en línea en https://www.europol.europa.eu/stopchildabuse.

133. En Bemba, una perita declaró sobre un informe elaborado por el "Human Rights in Trauma Mental Health Laboratory", que ella dirigía; Decision on requests to present additional evidence and submissions on sentence and scheduling the sentencing hearing, Bemba (ICC-01/05-01/08-3384), Sala de Primera Instancia III, 4 de mayo de 2016, § 13.

134. Koenig, supra nota 128, en 39–40; Koenig y Freeman, supra nota 10, pp. 340–341.

135. Koenig, supra nota 128, en 39–40. Véase también R v. Robb, donde un fonetista presentó prueba pericial, mientras que los agentes de policía que escucharon las mismas grabaciones impugnadas y reconocieron la voz de quien hablaba como la del acusado fueron considerados testigos fácticos.

136. Véase Amy Hak Forensics Report, supra nota 36, pp. 80–81.

137. Véase Al Hassan 15 October Trial Transcript, supra nota 106, p. 6.

138. R v. Bowman [2006] EWCA Crim 417.

139. Véase R v. Pabon [2018] EWCA Crim 420.

140. R v. Pabon [2018] EWCA Crim 420, § 58.

141. Véase supra nota 111.

142. Véase Decision on Defence Rule 94bis Notice Regarding Prosecution Expert Witness Richard Butler, Popovic et al. (IT-05-88-T), Sala de Primera Instancia II, 19 de septiembre de 2007, §§ 26–27; Popovic Butler Appeals Decision, § 31 (con ulteriores referencias jurisprudenciales).

143. Decision on Prosecution Request for Certification of Interlocutory Appeal of Decision on Admission of Witness Philip Coo's Expert Report, Milutinovic et al. (IT-05-87-T), Sala de Primera Instancia III, 30 de agosto de 2006, § 1.

144. Koenig y Freeman, supra nota 131, p. 1240.

145. Véase, por ejemplo, Amnesty International, "Myanmar: "Bullets rained from the sky": War Crimes and Displacement in Eastern Myanmar", 31 de mayo de 2022, disponible en línea en https://www.amnesty.org/en/documents/asa16/5629/2022/en/.

146. Véase Dwyer, supra nota 62, p. 78; Appazov, supra nota 5, p. 17 (señalando que "en el siglo XVII, los pensamientos de un testigo sobre un caso —su opinión sobre el caso, en contraste con los hechos establecidos— eran inadmisibles [en el derecho común]").

147. El modelo tradicional del crisol hacía a cada testigo personalmente responsable de la exactitud de su relato basado en su

experiencia sensorial. Por el contrario, la DOSI implica que múltiples personas capturen, editen, transfieran y posiblemente comenten el material, sin haberlo experimentado directamente por sí mismas en ningún sentido convencional.

148. Véase M. Gillett, "Fact-Finding Without Rules: Habermas's Communicative Rationality as a Framework for Judicial Assessments of Digital Open-Source Information", 44 Michigan Journal of International Law (2023) 301–348.

149. Véase Lubanga Trial Judgment, supra nota 31, § 112.

150. Véase G. Fiorella, "How to Maintain Mental Hygiene as an Open Source Researcher", Bellingcat, 23 de noviembre de 2022, disponible en línea en https://www.bellingcat.com/resources/2022/11/23/how-to-maintain-mental-hygiene-as-an-open-source-researcher/.

151 Véase W. Fan, "How to Organize a Collaborative OSINT Project for Litigation Purposes: Takeaways from Project Tollgate", University of Essex Human Rights Centre Blog, 26 de mayo de 2022, disponible en línea en https://hrcessex.wordpress.com/2022/05/26/how-to-organize-a-collaborative-osint-project-for-litigation-purposes-takeaways-from-project-tollgate/.

152 Trevisan, supra nota 26, nota al pie 8, citando L. Laving, "The Reliability of Open-Source Evidence in the International Criminal Court", Lund University Faculty of Law, 11 de junio de 2014, disponible en línea en https://lup.lub.lu.se/student-papers/search/publication/4457910. Véase también Berkeley Protocol, p. 8: "La fiabilidad se refiere a la capacidad de actuar de manera constante, fiable o según lo esperado"; Minogue, Allen y McDermott, supra nota 2, § 116.

153 Véase también Judgment on the appeal of Mr Bosco Ntaganda against the decision of Pre-Trial Chamber II of 18 November 2013 entitled "Decision on the Defence's Application for Interim Release", Ntaganda (ICC-01/04-02/06-271-Red), Sala de Apelaciones, 5 de marzo de 2014, §§ 36, 39–43.

154 Véase Amy Hak Forensics Report, supra nota 36, pp. 80–81.

155 Véase B. Wille, "'Video Unavailable': Social Media Platforms Remove Evidence of War Crimes", Human Rights Watch, 10 de septiembre de 2020, disponible en línea en https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes.

156 Decision on the "Prosecution Request for Disclosure of Material Underlying the Defence Psychiatric Expert Report", Ongwen (ICC-02/04-01/15-709), Sala de Primera Instancia IX, 21 de febrero de 2017, § 12. Véase también, por ejemplo, Regla 94bis del Reglamento de Procedimiento y Prueba del TPIY; Regla 94bis del RP&P del TPIR; Regla 116 del RP&P del Mecanismo; Singh, supra nota 56, pp. 627.

157 Bemba et al. Witness Exclusion Decision, supra nota 68, § 16.

158 Singh, supra nota 56, pp. 628–630.

159 International Bar Association, supra nota 48, p. 27. Aunque los jueces permitieron su presentación, en otras circunstancias podría adoptarse un enfoque diferente, especialmente si se tratara de una prueba fundamental que sustenta una condena.

160 Berkeley Protocol, §§ 153–175.

161 Ya se han rechazado pruebas en procedimientos ante la CPI cuando provenían de un URL que no podía recuperarse; véase Decision on the submission as evidence of items used during the questioning of witnesses but not submitted as evidence by the parties or participants, Bemba (ICC-01/05-01/08-3034), Sala de Primera Instancia III, 7 de abril de 2014, § 63.

162 Véase, por ejemplo, Hunch.ly, una herramienta de captura de sitios web ampliamente utilizada por investigadores digitales para tomar automáticamente capturas de pantalla y anotar páginas visitadas durante una sesión de investigación.

163 Véase L.B. de Chazournes, "Introduction: Courts and Tribunals and the Treatment of Scientific Issues", 3 Journal of International Dispute Settlement (2012) 479–481.

164 Gillett, supra nota 148.

165 F. Sampson, "Intelligent evidence: Using Open Source Intelligence (DOSI) in Criminal Proceedings", 90 The Police Journal: Theory, Practice and Principles (2017) 55–69, p. 61.

166 Véase, por ejemplo, Katanga and Ngudjolo Bar Table Motions, supra nota 78, § 29; Decision on the confirmation of charges, Mbarushimana (ICC-01/04-01/10-465-Red), Sala de Cuestiones Preliminares I, 16 de diciembre de 2011 ("Mbarushimana Confirmation Decision"), § 78.

167 Katanga and Ngudjolo Bar Table Motions, supra nota 78, § 31.

168 Mbarushimana Confirmation Decision, supra nota 166, § 40; CPI: Gbagbo Confirmation Adjournment, supra nota 82, § 29.

169 Opinión disidente de la Jueza Christine Van den Wyngaert, Judgment on the appeal of Mr Bosco Ntaganda against the decision of Pre-Trial Chamber II of 18 November 2013 entitled "Decision on the Defence's Application for Interim Release", Ntaganda (ICC-01/04-02/06-271), Sala de Apelaciones, 5 de marzo de 2014, § 4.

170 Judgment, Krstić (IT-98-33-T), Sala de Primera Instancia, 2 de agosto de 2001, § 108.

171 Al Hassan 15 October Trial Transcript, supra nota 106, pp. 33, 35–36.

172 Véase el contrainterrogatorio de Andras Riedlmayer en el caso Šešelj: Public Transcript of Hearing, Šešelj (IT-03-67), Sala de Primera Instancia, 27–28 de mayo de 2008.

173 Al Hassan 15 October Trial Transcript, supra nota 106, pp. 37–38.

174 Public Transcript of Hearing, Mladić(IT-09-92), Sala de Primera Instancia, 13 de agosto de 2015, 37746–37747; ICC-02/04-01/15-T-20-Red-ENG WT 21-01-2016 1/83 SZ PT, Ongwen (ICC-02/04-01/15-T-20-Red-ENG), Sala de Cuestiones Preliminares II, 21 de enero de 2016, p. 44, líneas 8–24; Decision on the confirmation of charges against Dominic Ongwen, Ongwen (ICC-02/04-01/15-422-Red), Sala de Cuestiones Preliminares II, 23 de marzo de 2016, § 51.

175 Al Hassan 15 October Trial Transcript, supra nota 106, p. 19 (también traducido como "refuerza" y "refuerza ligeramente").

176 Véase Hellwig, supra nota 14, pp. 984–986.

177 Véase da Silva, supra nota 2, pp. 960–962; Hellwig, supra nota 14, p. 987. Véanse infra los procesos de enmienda en la CPI.

178 MacLean, supra nota 16, p. 86.

179 Véase Hellwig, supra nota 14, pp. 986–987; R. Stoykova, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence', 42 Computer Law & Security Review (2021), p. 12.

180 Los tribunales estadounidenses establecieron en Daubert que, además de poseer los "conocimientos científicos, técnicos o especializados que ayuden al juzgador de los hechos a comprender la prueba o a determinar un hecho controvertido", los expertos deben cumplir un test preliminar de cuatro elementos relativo a su metodología y conclusiones: (1) ¿es falsable o comprobable el objeto del dictamen pericial?; (2) ¿se deriva este dictamen de técnicas con tasas de error conocidas (también formulado como "¿es el dictamen producto de principios y métodos fiables")?; (3) ¿ha sido sometido el dictamen a revisión por pares?; y (4) ¿ha sido aceptado este dictamen en la comunidad científica en general? Los principios de Daubert fueron posteriormente codificados en las Federal Rules of Evidence, fusionando los criterios de pertinencia y fiabilidad.

181 En el derecho del Reino Unido, el tribunal puede considerar los siguientes factores al determinar la fiabilidad de un experto propuesto: la naturaleza de los datos en los que se basa la opinión del experto; la solidez o fragilidad de las inferencias extraídas; la naturaleza de los métodos utilizados; el grado en que el material en el que se basa la opinión del experto ha sido sometido a revisión por pares; el grado en que la opinión se basa en material que excede el propio ámbito de especialización del experto; y si los métodos empleados por el experto siguen prácticas establecidas en el campo. Véanse las Criminal Practice Directions2015 [2015] EWCA Crim 1567, § 19A.5, citadas en Minogue, Allen y McDermott, supra nota 2, § 33.

182 Véase, por ejemplo, la Sentencia conforme al Art. 74 del Estatuto, Bemba (ICC-01/05-01/08-3343), Sala de Primera Instancia III, 21 de marzo de 2016, § 233; Sentencia de juicio en Lubanga, supra nota 31, § 112.

183 Véase supra la Sección 3.

184 Véase supra la Sección 3.

185 Dicho material podría afectar la credibilidad de la prueba de la Fiscalía y, por tanto, estaría sujeto a divulgación obligatoria por parte de ésta conforme al Art. 67(2) del Estatuto de la CPI. Alternativamente, constituiría "información pertinente para la preparación de la defensa" y, en consecuencia, debería revelarse conforme a la Regla 77, salvo que se aplicara alguna excepción.

186 Véase supra, Sección 4.A, sobre las cualificaciones generales de DOSI.

187 Véase supra, Sección 4.A.

188 Véase Semanza Appeal Judgment, supra nota 64, § 303; la decisión de la jueza Korner, resumida en Minogue, Allen y McDermott, supra nota 2, § 80. Véase también Bingham LJ en R v. Robb (sosteniendo que el fonetista estaba "bien calificado por su formación académica y experiencia práctica para expresar una opinión sobre la identificación de voces. No dudamos de que su juicio, basado en una atención cuidadosa a la calidad y el tono de la voz y a la pronunciación de vocales y consonantes, tendría un valor significativamente mayor que el del lego sin instrucción, del mismo modo que el juicio de un perito en grafología es superior al del ciudadano común").

189 Los expertos en DOSI pudieron señalar que, aunque Rusia tenía razón al afirmar que los metadatos mostraban el 16 de julio de 2014 en un video clave un día antes de lo esperado, ello se debía a que "en el momento en que se subió el video en 2014, un error en la estructura de un algoritmo de conversión de formato de video de código abierto utilizado por Google provocaba que los videos se cargaran con una marca temporal anterior en aproximadamente 24 horas al momento real de subida. De hecho, hasta 2019, todos los videos subidos a YouTube el 17 de julio de 2014 llevaban en sus metadatos una marca temporal del 16 de julio de 2014"; véase Bellingcat, supra nota 21.

190 Véase Decision on Defence Preliminary Challenges to Prosecution's Expert Witnesses, Ntaganda (ICC-01/04-02/06-1159), Sala de Primera Instancia VI, 9 de febrero de 2016, § 9. Véase también Sentencia de primera instancia, Ongwen (ICC-02/04-

01/15-1762-Red), Sala de Primera Instancia IX, 4 de febrero de 2021, § 2531.

191 Minnesota Supreme court decision of Keegan v. Minneapolis & St Louis Railroad cited in Milroy, citada en Milroy, supra nota 65, p. 520.

192 Véase Protocolo de Berkeley, supra nota 11, pp. 11–13.

193 Véase, por ejemplo, Criminal Practice Directions 2015 [2015] EWCA Crim 1567, § 19A.5, citado en Minogue, Allen y McDermott, supra nota 2, § 33.

194 Véase Jones v. Kaney (2011) UKSC 13, citado en Milroy, supra nota 65, p. 526.

195 Véase supra Sección 4.A.

196 D'Alessandra y Sutherland, supra nota 10, p. 14; Wiley, supra nota 98, p. 547.

197 Singh, supra nota 56, p. 645.

198 Véase CPI, "Experts", supra nota 59, p. 2.

199 Reglamento 24, Regulations of the Office of the Prosecutor (ICC-BD/05-01-09), 23 de abril de 2009.

200 Véase, por ejemplo, Al Hassan 15 October Trial Transcript, supra nota 106, p. 58.

201 Vecellio Segate, supra nota 13, p. 255.

202 Véase N. Milaninia, "Biases in Machine Learning Models and Big Data Analytics: The International Criminal and Humanitarian Law Implications", 102 International Review of the Red Cross (2021) 199–234. Véanse también Minogue, Allen y McDermott, supra nota 2, §§ 98–102; McDermott, Koenig y Murray, supra nota 2, p. 6; D. Simon, In Doubt: The Psychology of the Criminal Justice Process (Harvard University Press, 2012), p. 38.

203 Decision on the Procedures to be Adopted for Instructing Expert Witnesses, Lubanga (ICC-01/04-01/06-1069), Sala de Primera Instancia I, 10 de diciembre de 2007, § 15.

204 Véase Milaninia, supra nota 202, pp. 199–234.

205 La CPI cuenta con una Junta Asesora Científica y una Junta Asesora de Tecnología, lo que debería facilitar interacciones y diálogos continuos con la comunidad especializada en DOSI. Véase Koenig, supra nota 128, p. 34.

206 Vecellio Segate, supra nota 13, p. 244.

207 D'Alessandra y Sutherland, supra nota 10, p. 24.

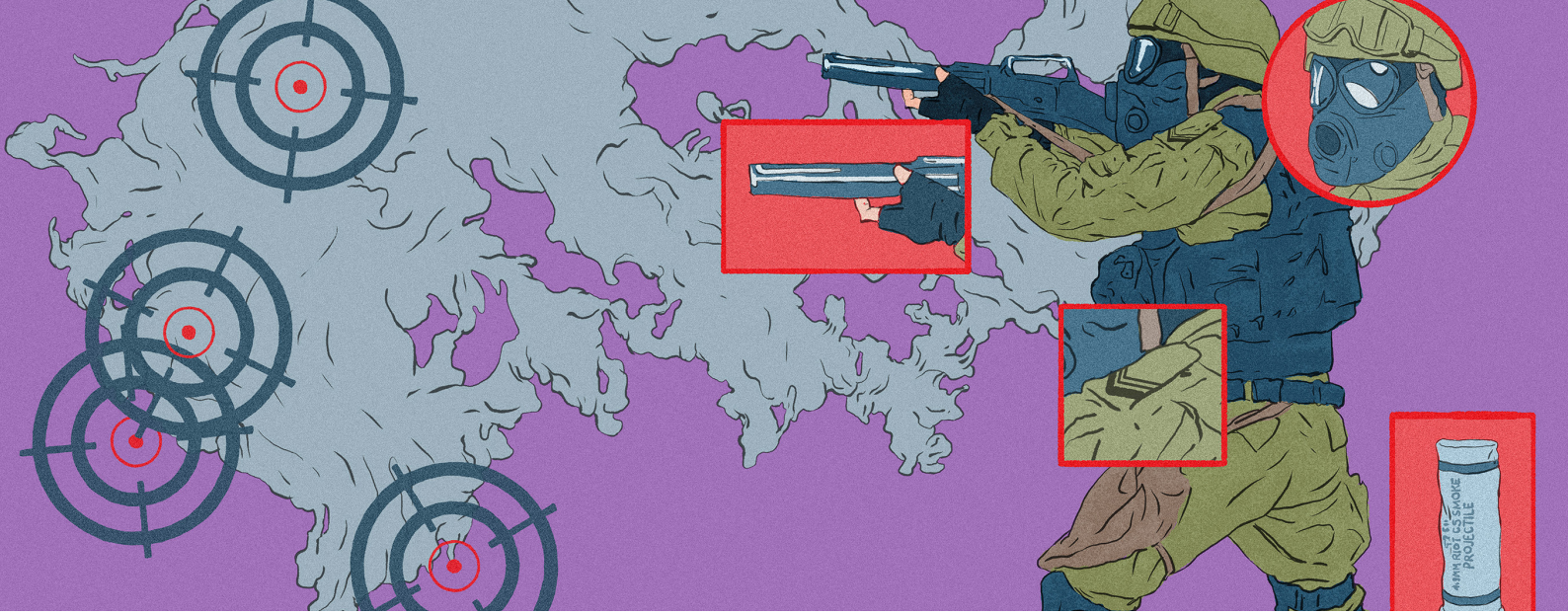
208 Véase, por ejemplo, D'Alessandra y Sutherland, supra nota 10.

209 Véase Richmond y Sebastiano, supra nota 5, p. 1027.

210 Véase Freeman y Vázquez Llorente, supra nota 23.

211 Review of the International Criminal Court and the Rome Statute System, ICC-ASP/18/Res. 7, 30 de septiembre de 2020, §§ 139–141; 554.

212 Véase supra Sección 3.




# El método Grillo: cómo reconstruir una verdad manipulada

La investigación que develó las irregularidades del ataque contra el fotorreportero Pablo Grillo sentó un precedente para la participación ciudadana organizada. Contra la prepotencia de un discurso oficial violento, el registro colectivo y multidisciplinario consiguió dar un salto en la disputa por la verdad. En este artículo te contamos cómo se articuló la reconstrucción forense que hizo tambalear a la versión oficial.

Facundo Cifelli - Luz Conde Vicente, integrantes del Mapa de la policía.

El miércoles 12 de marzo de 2025, en el marco de una nueva manifestación convocada por jubilados, se llevó adelante una escalada en la violencia estatal aplicada a partir del protocolo antipiquetes, la bandera de la represión enarbolada por la ministra de Seguridad, Patricia Bullrich. Ese día, hubo 114 detenidos y cientos de heridos, lo que convirtió la calle en una verdadera batalla campal.

Los casos más resonantes fueron el de Beatriz Blanco, una jubilada a la que la Policía Federal empujó y luego golpeó en el piso –el video del momento circuló mucho por las redes sociales–, el de Jonathan Navarro –quedó ciego de un ojo tras recibir el proyectil de una bala de goma que podría haber sido disparado por un efectivo de la Prefectura–, y el de Pablo Grillo, fotógrafo al que lo impactó un cartucho de gas lacrimógeno en la cabeza y lo dejó al borde de la muerte.

## La historia oficial

La versión oficial sobre el caso Pablo Grillo amontonó declaraciones apresuradas que demostraron de inmediato lo complejo que le estaba resultando al Gobierno salir limpio de esta situación. En esa fisura es que surge la posibilidad de reconocer la potencialidad política de plantear otro discurso basado en datos y pruebas.

El día de la represión, mientras Pablo recibía las primeras atenciones médicas, Patricia Bullrich habló

en La Nación +, con la conducción de Luis Majul. "Es un militante kirchnerista y está preso",dijo la ministra, lo que fue rápidamente desmentido por los allegados del herido. El 13 de marzo, al otro día, la funcionaria volvió a dar una entrevista en el mismo canal, pero esta vez en el programa de Cristina Pérez. Esta vez aseguró que "el miembro de una fuerza de seguridad tiró el disparo como dicen los manuales y la granada rebotó en el piso o en una barricada que ellos mismos habían armado antes" de impactar en el cuerpo del fotógrafo. Luego, habló con José del Río de vuelta en LN+, donde insistió con la idea de los dos rebotes. Es importante reconocer la articulación en la instalación de esta versión: ninguno de los entrevistadores cuestionó estos dichos aunque, a todas luces, carecían de sustento.

## La otra historia

Para entender el caso, es importante comenzar algunos días más atrás. El 26 de febrero se viralizaron las imágenes de Carlos, un jubilado hincha de Chacarita, siendo golpeado por las fuerzas de seguridad. La casaca que llevaba, un símbolo de identidad colectiva, fue el puntapié inicial para que más ciudadanos reconocieran la necesidad de apoyo. Su club fue el primero que convocó a acompañarlos y luego se sumaron otros con una frase cruda y maradoneana: "Hay que ser muy cagón para no defender a los jubilados".

El 11 de marzo, con la convocatoria hecha para el día siguiente, el Ministerio de Seguridad emitió el comunicado oficial titulado "Marcha de las Barras Bravas en las inmediaciones del Congreso de la Nación". En el texto, se avisaba que se implementarían "estrictas medidas para garantizar el orden y la seguridad pública".

El miércoles 12 de marzo, el equipo del Mapa de la Policía estaba reunido desde las 14:00 en las inmediaciones del Congreso para seguir de cerca lo que ya se anticipaba como una jornada marcada por la violencia. El objetivo, como en otras ocasiones similares, era monitorear lo que transmitían los canales de televisión en vivo, mientras llegaban las imágenes de la propia cobertura. Ni bien se conoció la existencia de un herido grave producto del impacto en la cabeza de un proyectil disparado por las fuerzas de seguridad, alrededor de las 17:30 horas, se decidió concentrar el trabajo en la investigación de ese episodio.

De esta experiencia participaron fotorreporteras/os, periodistas, videastas, peritos, diseñadores y numerosas personas que poseen diferentes saberes. Muchos de ellos nucleados en Mapa de la Policía y Archivo Histórico Orgánico de la Represión en Argentina (A.H.O.R.A.), pero también otros y otras que aportaron material a este caso particular. De manera coordinada se llevó a cabo una recolección masiva de imágenes, que fueron almacenadas y luego analizadas: la estructuración del material, su ubicación en tiempo y espacio y la sincronización para una idea general y detalles del suceso.

Los resultados de la experiencia se publicaron en dos partes, una a horas del hecho y otra a tan solo 4 días. Cuando se le consultó a la ministra Patricia Bullrich sobre esto contestó: "Las reconstrucciones que están haciendo no cumplen con los protocolos de las fuerzas de seguridad y no tienen análisis rigurosos".

## El método

Lo primero que llegó fue un video de un cronista de FM La Tribu –medio de comunicación que forma parte del Mapa de la Policía– donde se veía con bastante precisión el impacto en Pablo Grillo. Fue en ese momento que los peritos Guillermo Pregliasco y Martín Onetto comenzaron a trabajar con base en el material y con el objetivo de reconstruir en pocas horas el recorrido del proyectil para dilucidar la

identidad del tirador. Mientras tanto, un grupo de analistas comenzó a indagar de qué tipo de granada se trataba y cuáles eran las indicaciones para su uso. Por otro lado, se llevó a cabo un pedido de colaboración que se publicó esa misma noche en las redes sociales del Mapa con una indicación bien precisa: tenían que haber sido capturados entre las 17:20 y las 17:30.

La convocatoria se viralizó rápidamente y permitió el acceso a una amplia cantidad de registros, entre los que se recibieron:

- Fragmentos de videos de las transmisiones televisivas;
- videos y fotos inéditos aportados por la ciudadanía;
- imágenes crudas de fotorreporteras/os;
- videos de drones independientes;
- las imágenes que estaban en la cámara de Pablo Grillo.

La combinación de todas estas fuentes permitió crear una suerte de panóptico: una reconstrucción precisa, multiperspectivista y sincrónica, que desarmaba cualquier versión dudosa e intento de manipulación de los hechos. El análisis cuadro por cuadro y los metadatos de los archivos permitieron la creación de secuencia visual del recorrido completo del disparo hasta su origen: una nube de humo donde se encontraban efectivos de Gendarmería y otras fuerzas. Y un dato clave: el disparo salió a las 17:18.

Al mismo tiempo, se determinó que la munición era un cartucho de gas lacrimógeno, cuyo uso está regulado: este tipo de proyectiles deben dispararse en un ángulo de 45 grados y nunca de forma directa al cuerpo, debido a su peso y letalidad. Se trata de un arma solo para uso disuasivo. Las fotos con las que se cotejaron los videos dio el dato preciso de que a esa hora y en ese lugar solo había efectivos de Gendarmería Nacional (GNA) y se encontró que, en los minutos previos, se disparó varias veces en inclinación horizontal hacia los manifestantes. Esto habla de una práctica sistemática y coordinada de un uso incorrecto de las armas no letales y no de un tiro aislado.

La geolocalización de los teléfonos celulares, la acústica de los disparos, la técnica de estadísticas, el análisis de paredes y pinturas, son algunas de las técnicas que se utilizaron en este trabajo. Estas metodologías se usaron en otras causas a lo largo de nuestra historia como la de Teresa Rodriguez (se hizo una reconstrucción acústica), lo sucedido en el puente Pueyrredón con Maximiliano Kosteki y Darío Santillán (reconstrucción acústica), la masacre de Trelew (se demostró que la versión del teniente Roberto Bravo era inconsistente con los hallazgos del lugar), entre otras.

En una segunda etapa, la reconstrucción fue aún más precisa gracias a la llegada de registros de las horas previas, donde se determinó que quien lanzó el tiro que le dio a Grillo tenía uniforme color caqui, diferente al verde que prima entre los demás efectivos. Varias imágenes coincidían en la caracterización: gafas polarizadas, máscara antigases en su rostro, insignias y parches en su brazo izquierdo, dos morrales cruzados en su espalda, un morral porta municiones en la pierna izquierda y su arma lanza gases.

Finalmente, una foto en alta calidad permitió un salto en la investigación: se trataba de, como indicaba la identificación que llevaba en el traje, el cabo primero Héctor Guerrero (Nº legajo: 103208) perteneciente a la unidad móvil Nª6 de la Sección de Empleo Inmediato (SEI). El jefe de ese destacamento es el comandante mayor, Héctor Ferreira, y reporta al jefe del Comando Región I de la provincia de Buenos Aires, el comandante general Marcelo Fabián Porra Melconian. El despliegue contó con la aprobación y supervisión del director nacional de la Gendarmería, el comandante general Claudio Miguel Brilloni, quien estuvo presente ese miércoles. Por último, Patricia Bullrich definió el encuadre general previo de confrontación.

## La publicación

Esta información se compartió en dos tramos: a pocas horas del hecho –13 de Marzo a las 15.49–, donde se expusieron los primeros datos mencionados como la hora exacta, el tipo de proyectil, el lugar desde donde salió el disparo y el modo sistemático de mal uso de las armas no letales. La segunda parte se publicó a cuatro días de la manifestación, y consistía en la identificación exacta del tirador y la cadena de mando a la que obedecía. Ambos videos elaborados por el realizador audiovisual Alejo Fraile en la dirección y edición y Micaela Minervini y Mario Santucho en guion y prensa.

La estructura del Mapa que se construyó desde su creación fue clave en la rapidez y simultaneidad con la que se trabajó en todas las áreas involucradas. Tanto es así que los medios se hicieron eco de esta investigación y varios miembros del dispositivo Mapa de la Policía fueron invitados a distintos programas de radio y televisión a contar la experiencia. Pero incluso en ese sentido ya existían canales de difusión propios: tanto la convocatoria para reunir material como los dos videos de reconstrucciones tuvieron una enorme viralización, lo que habla de toda una masa de activismo que en Argentina que, a pesar de los esfuerzos del Gobierno, no se desactiva.

Sobre esto habla el físico forense e investigador del CONICET Guillermo Pregliasco, quien fue clave en esta investigación. En el episodio "De regreso a diciembre" del podcast del Mapa de la Policía, Pregliasco explica: "Es cierto que de cada hecho que ocurre en la vía pública cada vez hay más material audiovisual y en vez de aclarar las cosas puede confundirlas aún más. Al menos que contemos con herramientas para organizarlas, estructurarlas y visualizarlas nuevamente. Por eso es fundamental desarrollar un esquema que tenga una pata en las bases de datos, que haya un sistema de anotación de los videos y que haya interfaces cómodas para que muchas personas puedan trabajar a la vez sobre la misma base audiovisual".

## Supervivencia y justicia

Pablo Grillo fue operado de urgencia para bajar la presión intracraneal; el impacto del cartucho de gas lacrimógeno le provocó traumatismo de cráneo grave, fracturas múltiples y pérdida de masa encefálica. Luego vinieron otras cinco intervenciones más, la mayoría de ellas para tratar una constante pérdida de líquido cefalorraquídeo producto del impacto y la fractura. Todo esto durante casi tres meses de internación en terapia intensiva del Hospital Ramos Mejía.

La familia del fotorreportero se presentó como querellante con la patrocinación del CELS y tomó la posta de informar el estado de salud. A 55 días del disparo, Pablo salió a tomar aire por los balcones del Hospital. Luego de su sexta operación, en la que le colocaron una válvula y un catéter para subsanar la pérdida de líquido cefalorraquídeo, Pablo fue visitado por peritos y expertos del cuerpo médico forense que iniciaron un trabajo ordenado por la jueza a cargo de la causa, María Servini de Cubría. Este peritaje constató que las lesiones ocasionadas por el disparo del gendarme pusieron en riesgo la vida de Pablo.

Finalmente, el lunes 2 de junio se anunció que Pablo sería dado de alta de la terapia intensiva del Hospital Ramos Mejía, y trasladado al Hospital de Rehabilitación Manuel Rocca. Allí se encuentra desde ese momento, en donde cursa una rehabilitación y proceso de adaptación a las secuelas.

## El Poder Judicial en movimiento

El Mapa de la Policía fue citado en la Justicia para mostrar el material desmenuzado que se usó para las reconstrucciones, un hito en la participación ciudadana, la organización popular y la resistencia al uso violento de las fuerzas de seguridad por parte del Estado. Por su parte, la Gendarmería Nacional cerró el expediente administrativo, lo que indicó que el cabo Guerrero siguiera en funciones y el informe atribuyó el disparo que puso en riesgo la vida de Pablo Grillo a un "hecho fortuito", producto de la mala visibilidad y de la imprudencia de la víctima por ubicarse "en la línea de tiro".

Luego de la presentación del informe del Mapa de la Policía sobre las reconstrucciones audiovisuales, el juzgado ordenó una pericia a cargo de la División Balística de la Policía de la Ciudad. Esta descartó por completo que el disparo de Guerrero hacia Grillo haya sido en 45 grados hacia arriba o entre los 30 y 45 grados hacia abajo, como exige el manual. También se verificó que si el disparo hubiese sido "en parábola" hacia arriba, hubiese caído tres veces la distancia en la que se encontraba Grillo respecto de Guerrero. Con este informe, además, se volvió a validar que lo dicho por la Ministra de Seguridad, Patricia Bullrich, también fue falso.

Luego, el juzgado citó a prestar declaración indagatoria al cabo Guerrero como autor del disparo que hirió de extrema gravedad a Pablo Grillo. El oficial aseguró que es inocente, que no tuvo la intención de lastimar y que usó el arma correctamente. Finalmente, la jueza Servini dictó el procesamiento, sin prisión preventiva, del cabo Héctor Guerrero por los delitos de lesiones gravísimas y abuso de armas reiterado todo agravado por ser miembro integrante de una fuerza de seguridad. También impuso un embargo a Guerrero de $203 millones y mantuvo la prohibición de salir del país.

La jueza validó las pruebas presentadas y se confirmó que Guerrero fue el autor material del disparo de la granada de gas lacrimógeno que hirió de gravedad a Pablo Grillo. La resolución del juzgado demuestra además que de todas las ocasiones en las que Guerrero disparó de forma antirreglamentaria, ninguno de sus jefes intervino para frenarlo.

*Esta reconstrucción se llevó a cabo con el material cedido, entre otros colaboradores, por Indymedia, Emmanuel Coria, Kaloian Santos Cabrera, Javier Aranciva, Enfoque Rojo Y La Izquierda Diario.*

Podés escuchar más detalles de la reconstrucción en los talleres de A.H.O.R.A. en el canal de Spotify del Mapa de la Policía.

PDF del informe completo presentado en sede judicial disponible aquí.

# Violencia en redes sociales y retos de la evidencia digital: a propósito del caso Julia Mengolini

Raisha Correa, Andrés Carbel y Joaquín Simbad Rapoport, integrantes de Equipo de Investigación Política*

*Este estudio es fruto de un trabajo colectivo y colaborativo*

*Queremos agradecer y nombrar a cada una de las personas y organizaciones que han colaborado en esta investigación: la mesa de violencia digital impulsada por la Fundación Boll; Camila de Argentina Humana; Nulo; Germán; Sol; Tes; Nico, Clari, Matias, Mario y Gabi, del Registro de Ataques de las Derechas Argentinas Radicalizadas (RA-DAR).*

## 1. El problema

La expansión acelerada de las tecnologías digitales desafía a la sociedad y sus instituciones. Nuevos patrones de comunicación e interacción, surgidos de la creciente participación en la esfera digital y redes sociales, permean todos los ámbitos de la vida cotidiana. **Ante vidas crecientemente virtualizadas, la idea misma de lo que se puede concebir como espacio público se redefine**, en la medida en que las plataformas algorítmicas de encuentro son propiedad de unas pocas megacorporaciones privadas, cuya finalidad principal es comercial.

El siguiente escrito se inscribe en este contexto, anclado en una experiencia singular: **la campaña virtual de difamación y el ataque coordinado contra Julia Mengolini**, la periodista feminista argentina y fundadora del medio digital Futurock. Allí cumplió un rol protagónico el presidente de la Nación argentina y un grupo de activistas, influencers, periodistas, políticos y funcionarios afines al partido de

*Equipo de Investigación Política (EdIPo) de la Revista Crisis y del Registro de Ataques de las Derechas Argentinas Radicalizadas (RA-DAR).

gobierno. El caso, que podemos catalogar como de "violencia digital" o "violencia en línea", ilumina una serie de fenómenos relativos a nuevas modalidades de violencia institucional facilitadas por la tecnología:

- **las redes sociales como plataforma para el escarnio público**, la realización de amenazas y campañas de hostigamiento público;
- **el involucramiento de funcionarios públicos en campañas de odio** y desinformación, que terminan por configurar nuevas formas de violencia institucional al habilitar un clima que legitima la violencia en la escena pública;
- **la dificultad habitual para identificar a responsables de ataques digitales**, en la medida en que proliferan los mecanismos de ocultamiento de identidad;
- **y el reto del acceso a la información y la cooperación de las plataformas digitales**, que dificultan la investigación de este tipo de hechos.

El caso permite reponer, además, al litigio estratégico colectivo y colaborativo como parte del repertorio de acciones disponibles para la resistencia a los embates de gobiernos autoritarios contra voces disidentes. En esta ocasión, la disputa en el terreno judicial transformó a la víctima de un ataque orquestado desde el centro del poder político, en una accionante que toma un papel activo en el procedimiento legal. En Argentina abundan las experiencias de víctimas que, en su búsqueda de verdad y justicia, asumieron una voz pública y contestaria para enfrentar la violencia política y exigir transformaciones institucionales. **Ante nuevas formas de violencia estatal, resulta propicio reflexionar sobre nuevas respuestas posibles**: los dispositivos digitales de captación, almacenamiento y análisis de información también son un recurso a la mano para la acumulación de evidencia detallada y precisa, que permite la apoyatura empírica de una verdad histórica por construir colectivamente.

# 2. El ataque a Julia Mengolini como caso testigo

Desde hace años, la periodista Julia Mengolini es **víctima de acoso y violencia digital en redes sociales**, principalmente en X (antes Twitter). La situación se intensificó con la llegada al poder del presidente Javier Milei, cuyo discurso hostil hacia el periodismo, las mujeres y el movimiento feminista generó un ambiente que normaliza los ataques digitales en todo su nivel.

A mediados de 2025, los episodios de violencia que sufría dieron un giro: **los ataques dejaron de ser sólo públicos y pasaron al ámbito personal**. La periodista empezó a recibir amenazas directas y de forma sistemática a través de Instagram, X, Telegram y correo electrónico. Las intimidaciones comenzaron tras la "viralización" de una noticia falsa (*fake news*) difundida por militantes, políticos, funcionarios e *influencers* afines a La Libertad Avanza, partido político del presidente Milei. Esta situación marcó un antes y un después en su experiencia con la violencia, provocándole una situación de miedo real y sostenido en el ejercicio de su profesión.

## Difusión de la noticia falsa

**El 20 de junio de 2025**, Mengolini **tomó conocimiento de una campaña digital organizada en su contra** tras leer una publicación en X de la diputada nacional por La Libertad Avanza (LLA), Lilia Lemoine, donde la involucraba en una relación incestuosa con su hermano.

Tras una revisión de publicaciones en forma cronológica en la red social X, se encontró que la **primera**

**publicación de la noticia falsa fue realizada el día 19 de junio de 2025 a las 15:37 hs.** El nombre de la cuenta era "Fer Oria" y su usuario @oriafer23, una cuenta con identidad falsa y sin aparente vinculación política. En el mensaje decía lo siguiente: "*¿Querés que hablemos de tu relación con tu hermano, Mengolini? Cuando se metían juntitos al lago como los hermanos de la película La Laguna Azul... Al final, la que está enamorada de su hermano sos vos*" (el subrayado es nuestro).

**La publicación del usuario @oriafer23 se extendió rápidamente en la red social**. Se sumaron muchas réplicas (retuits) y comentarios, sobre todo de simpatizantes, activistas y militantes afines al partido oficialista, exacerbando su contenido original. Tanto cuentas con pocos seguidores, así como actores digitales con alcance masivo en la red social y reconocidos por su cercanía política al presidente. Por ejemplo, el abogado Sarubbi Benitez, conocido en el universo Twitter como @GordoLeyes. Solo el retuit de Sarubbi, que daba entidad de "carpetazo" al rumor, generó alrededor de **115 mil visualizaciones en menos de 48 horas.**

**El 19 de junio a la tarde**, la noticia falsa sobre Mengolini y su hermano se había extendido en el universo de activistas y militantes del partido LLA, quienes replicaron la noticia con el afán de humillarla y exponerla públicamente. Esto generó que la periodista decidiera poner en privado su cuenta de X, con el fin de limitar las menciones y la oleada de mensajes que le empezaban a llegar por diferentes redes de mensajería.

A pesar de la restricción de su cuenta principal, la *fake news* continuó expandiéndose. La cuenta anónima @TTendenciaX —cuenta verificada afín a la militancia libertaria y con más de 47 mil seguidores, conocida por instalar noticias sensacionalistas, falsas y difamatorias— publicó al cierre del día: "*Julia Mengolini": Porque tras descubrirse que sostuvo una relación incestuosa con su hermano, puso en privado sus redes*". **El mensaje difamatorio alcanzó 1.7M visualizaciones y tuvo más de 24 mil likes en menos de 24 horas.**

## Acoso digital con tolerancia estatal

Julia Mengolini decidió alejarse de las redes sociales por algunos días, a fin de salvaguardar su salud física y emocional, así como también evaluar medidas legales y discursivas frente al ataque coordinado que estaba siendo víctima. También creía que la violencia que convocaba a los simpatizantes y militantes libertarios cesaría pronto. Sin embargo, el ensañamiento no cesó. Todo lo contrario, las estrategias de violencia digital fueron más crueles y siniestras.

**El 24 de junio de 2025** se viralizó un audio que la periodista compartió con su colega argentina Nancy Pazos. Allí se escuchaba a Mengolini totalmente conmocionada con la situación. Ese mismo día se viralizó un clip de su programa de radio, "Segurola y Habana", donde la periodista le consultó a un abogado qué medidas podría tomar al respecto. La situación generó una reacción inmediata por parte de la militancia libertaria, quienes la acusaron de hipocresía y de "no bancarse el vuelto". **El presidente Javier Milei compartió algunas de esas publicaciones y en una de ellas agregó el siguiente mensaje**: "*DECIME QUE SOS PARTE DEL PERIODISMO BASURA SIN DECIRLO. Parece que cuando ella pega con sus mentiras está bien pero cuando le viene el vuelto llora y quiere ir a la justicia... Fin. PD: PN°10(E)*" (el subrayado es nuestro).

PN°10 (E) significaría: cosecharás lo que siembras. Mientras que, la "devolución de un vuelto" es en referencia a la supuesta vinculación amorosa que habría hecho la periodista entre el presidente y su hermana, quien había afirmado en un programa de televisión emitido en agosto de 2024 por C5N que él debía estar "enamorado" de su hermana, una declaración que después aclaró negando cualquier

insinuación de incesto.

## Ataque coordinado de deepfake sexual

**Tan solo un par de horas después del mensaje amenazante del presidente**, con una foto familiar que tenía la periodista en su cuenta de Instagram, cuentas anónimas y con identidad falsa afines a la militancia libertaria generaron con inteligencia artificial (IA) un video donde aparece besándose con su hermano. El video se difundió de forma masiva inmediatamente, y a partir de ahí, siguieron con otras escenas de carácter sexual y miles de comentarios y mensajes agresivos en todas sus cuentas.

**El ataque que más perturbó a la periodista llegaría horas más tarde**. La cuenta de X Pedro María Lantaron, con nombre de usuario @elpittttt, **publicó un mensaje asegurando tener un supuesto video íntimo de Julia Mengolini y su hermano**, prometiendo enviarlo por mensaje privado a toda persona que se lo solicite.

Desde ese momento, empezó la difusión de varias publicaciones en X haciendo referencia al supuesto vídeo de carácter sexual, que habría sido generado con IA generativa (deepfake). No importaba si el video era creíble o no, y tampoco si existía o solo era la instalación de una noticia difamatoria. **El objetivo era claro: instalar la idea de su existencia para ridiculizar, insultar y eliminar del entorno digital a la periodista.**

**El 25 de junio de 2025**, el mismo usuario @elpittttt, compartió una falsa carta documento, en la que se insinuaba que Mengolini reconocía la autenticidad del video y solicitaba que lo eliminen porque formaba parte de su intimidad sexual. Esta nueva noticia falsa —compartida y viralizada por diversas cuentas libertarias— intensificó el hostigamiento contra la periodista.

**El ataque en redes continuó, a lo que se sumaron mensajes con amenazas de carácter sexual y de muerte hacia Mengolini**. Diputados nacionales y provinciales libertarios, periodistas, funcionarios públicos y hasta el propio presidente se sumaron a esta segunda oleada de violencia. El caso también llegó hasta los medios de comunicación, donde el hecho fue espectacularizado de forma banal y totalmente revictimizante.

A raíz de estos últimos ataques digitales, **la periodista comenzó a sufrir graves afectaciones en su salud emocional, una situación que no había vivido nunca como periodista**. La violencia había traspasado el plano virtual y comenzó a afectar su vida diaria.

**El 28 de junio de 2025**, la diputada libertaria Lilia Lemoine, el diputado provincial Agustín Romo y el director de Realizaciones Audiovisuales de la Presidencia, Santiago Oria, publicaron nuevos mensajes burlándose del caso. El relato de la "devolución del vuelto" continuaba.

**Hasta el 30 de junio de 2025**, el presidente Javier Milei había acumulado 93 publicaciones atacando a la periodista Julia Mengolini. Un día antes, en una entrevista televisiva en el canal de *streaming* "Neura" habló por primera vez del tema fuera de las redes sociales. Se defendió diciendo que los periodistas atacaban siempre a la militancia de la Libertad Avanza, que Julia Mengolini era parte de un grupo de "enemigos" y que no era más que una "zurda de mierda". Con esta declaración, el presidente no solo justificaba los ataques digitales, sino que también construía un discurso de enemistad y eliminación contra la periodista de forma pública.

## La violencia estatal avanza

El entramado de miles de cuentas trolls, militantes libertarios, dirigentes nacionales y provinciales, funcionarios públicos y hasta el propio presidente de la Nación, evidencia **nuevas formas de violencia estatal y paraestatal que urgen reconocer para empezar a enfrentarlas: resulta claro que componen un dispositivo complejo de acción coordinada.**

Las campañas de violencia digital contra periodistas críticos al gobierno, nos demuestran una construcción de la enemistad que pone en peligro pilares fundamentales de la democracia tales como la libertad de expresión y la construcción de una esfera pública respetuosa o al menos pacífica para el intercambio de diferencias. Si bien hay otros casos de ataques a periodistas similares, cabe resaltar el innegable factor de género en estos hechos. La mayor parte de estos ataques digitales se dirigen a periodistas mujeres y feministas.

La violencia que sufrió la periodista Julia Mengolini no es un hecho aislado. Diversos colectivos denunciaron agresiones provenientes de funcionarios públicos, diputados y personajes cercanos al oficialismo. El colectivo "Periodistas Argentinas" presentó un informe sobre cómo el *trolleo* oficial se utiliza como mecanismo de censura contra periodistas mujeres y feministas. Un 80% de las periodistas censadas señaló sentirse inhibida de manifestarse en redes por temor al acoso y los ataques, mientras que un tercio debió de cambiar de trabajo por esa violencia.

Todo este engranaje de violencia digital legitimado desde las más altas esferas del poder se defiende bajo la épica de una "batalla cultural". "Batalla cultural" que, según afirman diversas investigaciones periodísticas, sería financiada con fondos públicos, a través de estructuras estatales como la Secretaría de Inteligencia de Estado (SIDE), con la conducción política del asesor presidencial Santiago Caputo. En esta misma red participa el tuitero "Juan Doe", director de Comunicación Digital del Gobierno, quien ocupa un rol central en la coordinación de lo que llamamos "milicias digitales".

Asimismo, la habilitación del discurso violento desde el Estado tiene consecuencias concretas: legitima públicamente la violencia y normaliza el ciberacoso hacia cualquier voz opositora al gobierno de turno. El caso de la periodista Julia Mengolini demuestra con crudeza cómo las **violencias digitales trascienden el ámbito virtual y se filtran en la vida cotidiana**, afectando incluso al entorno familiar y laboral.

El debate sobre las violencias en las redes sociales no es solo un tema que incumbe a las plataformas digitales, es también sobre las estructuras de poder que la sostienen y legitiman, aunado **a las pocas herramientas del sistema de justicia para actuar de oficio en este tipo de casos y brindar respuestas efectivas a las víctimas del poder político.**

## Algunas preguntas en torno al caso

Los desafíos planteados en el problema se transforman en preguntas que requieren ser abordadas específicamente:

1. **¿Bajo qué marcos interpretativos resulta más adecuado encuadrar una campaña pública que trasciende las fronteras de la "violencia simbólica"?** Es sabido que los discursos de odio influyen en la estigmatización de actores y generación de mayores niveles de polarización, lo cual políticamente se vuelve un obstáculo para la convivencia democrática. Sin embargo, en los últimos años observamos que este marco resulta insuficiente para dar cuenta de campañas que no sólo buscan este efecto, sino que además apuntan coordinadamente

y sistemáticamente a blancos específicos que permitan canalizar el enojo social. Se trata de campañas que instigan a la violencia de forma directa, organizadas en red y que no solo buscan expresar ideas sino silenciar voces.

2. **¿Cómo identificar a quienes promueven y difunden discursos de odio o amenazan a otras personas en el ámbito digital?** Las cuentas utilizadas para enviar los mensajes más violentos habitualmente son perfiles falsos o cuentas anónimas, muchas veces de corta duración y marginales. De esta manera, y con la reticencia a colaborar con la institución judicial por parte de las plataformas tecnológicas, resulta difícil, cuando no imposible, responsabilizar a quienes realizan estas acciones por detrás de sus avatares virtuales. Aquí no solo se trata de la opacidad con que se actúa, sino también de la velocidad, que muchas veces resulta determinante para volver estériles los pedidos de información judiciales.

3. **¿Cómo probar la participación de actores estatales o con aquiescencia estatal en la planificación y ejecución de estos ataques?** En nuestro país, la ultraderecha encontró en estas campañas un modus operandi habitual, ampliamente discutido en los medios de comunicación e insólitamente reconocido por personajes influyentes del propio gobierno. Sin embargo, es difícil probar la participación o el financiamiento institucional de estas campañas, y demostrar la utilización de materiales y recursos estatales. Más allá de trascendidos e indicios, resulta fundamental para comprender la real magnitud del fenómeno.

# 3. Enfrentar la violencia, demandar justicia

Un par de semanas después de la campaña de intimidación coordinada, **la periodista presentó una denuncia penal contra el presidente**, funcionarios de turno, activistas libertarios, *influencers* y usuarios de redes sociales de IG y X que participaron en los diversos ataques digitales que sufrió desde el 19 de junio de 2025. La denuncia fue por amenazas, intimidación pública e incitación al odio, malversación de fondos y asociación ilícita destinada a combatir ideologías e imponer sus ideas por la fuerza. A raíz de ello, el Juzgado que intervino le otorgó medidas de protección, que incluyeron custodia policial y botón antipánico, al considerar que existía un riesgo cierto y real para su integridad física y psíquica.

## De caso individual a causa pública

Una denuncia penal puede interpretarse como algo más que un hecho administrativo o un pedido de reparación que importa exclusivamente a quien reclama justicia. De hecho, quienes no están inmiscuidos en asuntos legales desconocen que la figura de la Fiscalía o Ministerio Público solo existe cuando hay delitos. Se instituyó porque determinadas infracciones se consideran lesivas no solo hacia los directamente afectados, sino hacia la sociedad toda. Por ello, una voz pública, en nombre de todos los que componen esa sociedad, se alza para acusar y exigir justicia. No lo mencionamos para reivindicar un rol justiciero para las fiscalías, sino para recordar que **muchas veces lo que se tramita por expedientes judiciales es asunto público y concierne a todos**.

El pasaje de Julia Mengolini, de víctima a querellante, implicó volver al caso un asunto público. A continuación, reseñamos brevemente la acción judicial presentada y la respuesta obtenida hasta el momento.

## De víctima a querellante

En principio, **la acción judicial realizada, se volvió una barrera o dique de contención para las prácticas violentas**, que hasta entonces se ejercían sin temor a represalia alguna. No solo por la denuncia en sí, sino porque se realizó acompañada de un alzamiento de la voz pública. Junto con el x|trámite ante los tribunales, que tuvo el patrocinio legal del referente político Juan Grabois y el respaldo de la organización social *Argentina Humana*, también se presentó el caso en una clase magistral de la Facultad de Derecho de la Universidad de Buenos Aires a través de la charla "Inteligencia artificial y violencia estatal", a la cual asistieron numerosos estudiantes, académicos, militantes políticos y funcionarios judiciales. Allí se lo presentó como un caso paradigmático, desde un enfoque técnico y político que permitiera apreciar que lo sucedido implicaba el cruce de un límite intolerable por fuera de los consensos para la vida democrática.

Además de invertir los términos —de víctima de una campaña de difamación, a acusadora; de ejecutores de la violencia, a posibles responsables de un delito—, **la denuncia permitió una pronta respuesta judicial**, con medidas tendientes a proteger la integridad física de la víctima. Si bien se puede hipotetizar que la publicidad del caso provocó una excepcional respuesta rápida, nos consta que en casos similares con menor repercusión la denuncia misma generó una mínima cobertura y reconocimiento de la situación de riesgo por parte del poder judicial.

## Investigación en fuentes abiertas y evidencia digital

**La recolección de la evidencia digital para la denuncia contó con la colaboración del Equipo de Investigación Política (EdIPo)**. El equipo jurídico de la organización *Argentina Humana* se propuso realizar una presentación con abundante prueba, hipótesis claras y bien fundadas, de modo tal que funcione como caso testigo y aporte a generar antecedentes favorables en la justicia. Esto dio por resultado una dinámica colaborativa por parte de un grupo amplio e interdisciplinario.

La recolección de evidencia apuntaba a desandar lo que, apenas un par de semanas después de iniciado el ataque, aparecía como una maraña confusa de mensajes en redes sociales. Para ello, **el primer paso fue un relevamiento minucioso de la red social X**, utilizando comandos de búsqueda avanzada: operadores de fecha, términos clave, uso de hashtag y monitoreo de cuentas que habitualmente participan en este tipo de ataques. Así se pudo identificar mensajes que funcionaron como hitos dentro de la campaña de difamación, así como los especialmente violentos. De esta manera, **logramos identificar a 20 cuentas que participaron del ataque**, seleccionadas por el contenido de mensajes especialmente violentos o por su relevancia pública y capacidad de amplificación en la red.

El análisis de estas cuentas permitió identificar un conjunto seleccionado de mensajes que era necesario preservar. Aunque algunos posteos particularmente relevantes ya no se encuentran disponibles más que en capturas de pantalla, **se logró preservar la prueba digital a través del sitio archive.today**, un portal que permite salvaguardar una copia de cualquier página en la web, con todas sus imágenes, estilos y fuentes.

**La participación del presidente Javier Milei resultó particularmente difícil de reconstruir**. Los usuarios en X tienen tres formas de generar contenido: 1) elaborar una publicación propia (*postear*, por *"to post"*, en inglés); 2) citar la publicación de otro con un comentario propio; 3) *repostear*, es decir, difundir la publicación de alguien más sin agregarle otro mensaje. A diferencia de otros usuarios, la cuenta oficial del presidente concentra la mayor parte de su actividad en *reposteos*. Contrario al posteo o

1. El reposteo no muestra de forma pública una ruta identificable y compartible para acceder desde otro ordenador. Es posible reconstruir a través de los metadatos de la publicación un enlace al reposteo, pero requiere de conocimientos técnicos específicos.

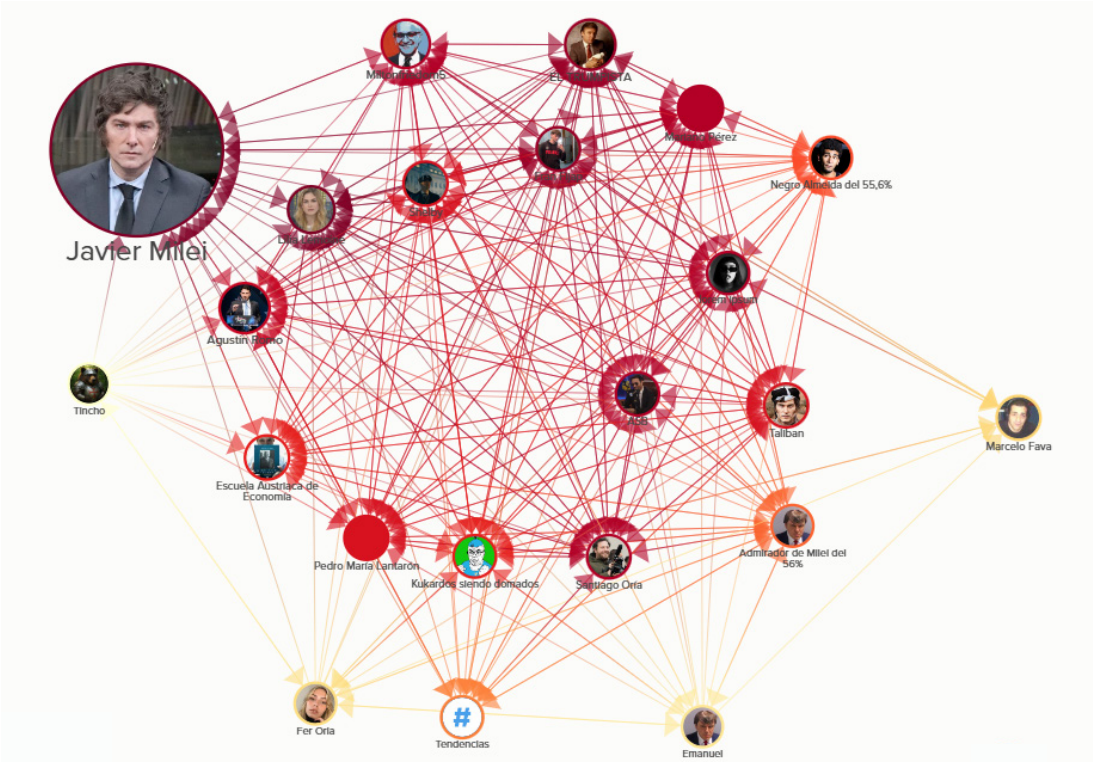
la cita, el *reposteo* no genera un nuevo enlace público[1], pero igualmente repercute en que los seguidores de la cuenta que hace el *reposteo* vean el contenido, junto con un mensaje que indica quién lo compartió.

**Para el análisis de la actividad realizada por la cuenta del presidente, se acudió a un sitio web que la monitorea de forma sistemática y a través de protocolos públicos: milei.nulo.lol**. Es desarrollado por un usuario que, a través de herramientas de código abierto, produce portales con información pública a disposición de todo el público en general. Entre otros, participó en proyectos para el monitoreo de precios de productos en sitios web, archivado de portales de datos abiertos y estadísticas de demoras de vuelos según la empresa aérea. Esta última iniciativa, *failbondi*, fue aceptada como prueba en una acción colectiva ante la justicia.

Una mirada al sitio permite mesurar el particular uso de la red social por parte del presidente Milei: del contenido compartido en su cuenta oficial durante octubre de este año, menos del 2% son posteos propios o citas a otros posteos, mientras que más del 98% restante consistió en *repostear* contenido producido por otras cuentas. A través de la plataforma, se pudo reconstruir que la participación del presidente en el ataque coordinado contra Julia Mengolini fue central. **Javier Milei realizó más de 100 posteos, volviéndose un componente clave para la expansión del hostigamiento hacia la periodista**.

Una vez reconstruida la actividad de la campaña difamatoria en X se realizó un análisis de redes. La técnica permite visualizar, a través de nodos y aristas, un conjunto de información vasta. Una matriz de datos reticular de este tipo está a la base de dispositivos tan diversos como el protocolo original de búsqueda de Google (*pagerank*), análisis etnográficos para reconocer relaciones de poder en comunidades, y la investigación de redes de criminalidad compleja. En este caso, se trató de un análisis preliminar que permite indicar la trama de **conexiones, inusualmente densa, entre las distintas cuentas que protagonizaron el ataque coordinado contra Mengolini**.

Para ello se utilizó la aplicación web Kumu, que permitió ubicar a las 20 cuentas identificadas en el relevamiento en una misma visualización: a) las cuentas responsables del ataque; b) la relación entre cuentas, realizada relevando "quién sigue a quién" dentro de la plataforma; c) el impacto potencial de cada cuenta, ponderando su tamaño según la cantidad de seguidores dentro de la plataforma; d) la




Ver visualización interactiva: https://kumu.io/asm/grafo-cuentas

centralidad de cada actor dentro de la red, ponderado según la cantidad de seguidores dentro de la red de cuentas seleccionadas.

Este **análisis preliminar resulta útil para identificar indicios de coordinación entre los actores involucrados**. En primer lugar, porque permite integrar numerosa información puntual en una visualización panorámica. En segundo lugar, porque la estructura de red inusualmente densa entre las cuentas expresa a un potencial grupo articulado y coordinado. Por último, porque el reconocimiento de las particularidades de cada actor también permite elaborar hipótesis sobre los roles diferenciados entre las cuentas. Mientras que los mensajes disparadores de la campaña y con los contenidos más violentos fueron realizados por cuentas relativamente marginales tanto en la red como en cantidad de seguidores, la amplificación y masificación de los mensajes corrió por cuenta de los actores centrales, con capacidad de llegada e instalación de agenda, quienes a su vez cumplen roles institucionales relevantes.

## Más allá de la demanda inicial

La denuncia interpuesta por los abogados y abogadas, en principio, prosperó con la imputación de los acusados. Superada esa primera barrera de admisión judicial, **los desafíos probatorios se concentran en dos cuestiones**: identificar a los responsables de las amenazas directas realizadas a la periodista y demostrar que hubo una pata política, con responsabilidades institucionales, que inició, ejecutó y coordinó la campaña de hostigamiento.

**En torno a la primera cuestión**, resulta determinante la identificación de usuarios reales detrás de los avatares virtuales, para lo cual se precisa la colaboración de las plataformas digitales a través de las cuales se realizaron las amenazas.

**La segunda cuestión reviste una dificultad mayor**, ya que requiere recolectar otro tipo de prueba que fundamente de forma sólida la responsabilidad del presidente y su círculo cercano en el diseño y ejecución como actores imprescindibles para el ataque. A su vez, en la medida en que la institución judicial funciona no solo por un proceder burocrático, sino también como un poder del Estado, requiere de la construcción de legitimidad pública para sustentar medidas y decisiones en tal sentido. En este sentido, **la querella se propuso incorporar a la causa a organismos de derechos humanos y periodísticos como amicus curiae**. Esta figura permite incorporar a terceros interesados en el avance de la investigación, mostrando a los funcionarios judiciales que la resolución del caso resulta relevante para otros actores sociales.

**El desafío ulterior es que lo avanzado en la etapa de instrucción sea refrendado por las etapas judiciales posteriores**, y en ese sentido la prueba debe trabajarse de forma meticulosa, para que sea considerada válida y suficiente también por las instancias superiores. De todos modos, a poco de andar este caso muestra que es posible diseñar una respuesta rápida y prometedora a la violencia estatal. Para ello, fue preciso alzar la voz pública, organizar el material digital disponible en fuentes abiertas (en este caso, en redes sociales), preservarlo, visualizarlo y analizarlo de forma tal que aporte a la identificación de los actores responsables de la violencia digital.

# 4. Lecciones y desafíos

Como lo muestra la experiencia analizada, la situación presenta desafíos múltiples que exceden al caso de la periodista Julia Mengolini. Dejamos, a continuación, un conjunto de cuestiones sobre las que creemos es necesario seguir reflexionando y explorando alternativas:

# 4.1 Desafíos en el ámbito técnico

## Limitaciones y desafíos de la investigación en fuentes abiertas

**La investigación en fuentes abiertas** —conocida como OSINT o DOSI[2]— **constituye un avance crucial para el análisis de la violencia digital** al permitir recolectar, sistematizar y analizar información pública proveniente de redes sociales, foros, sitios web y metadatos sin vulnerar sistemas cerrados ni recurrir a técnicas invasivas. **Su potencial radica en transformar la sobreabundancia de datos en evidencia verificable y jurídicamente utilizable**, habilitando la reconstrucción de hechos y la atribución de responsabilidades a partir de huellas digitales dispersas. No obstante, su implementación enfrenta algunos retos significativos:

- Acceso y preservación de la evidencia digital (contenido efímero, borrado o manipulado).
- Identificación de usuarios anónimos (cuentas falsas o *bots*).
- Límite entre análisis de fuentes abiertas y herramientas que requieren órdenes judiciales.
- Dificultad para preservar metadatos imprescindibles para validar evidencia.
- Limitaciones para analizar evidencia multimedia (detección de edición o *deepfakes*).
- Necesidad de la validación metodológica: el hecho de que un dato sea público no garantiza su valor probatorio ni su legitimidad de uso.
- La gestión del consentimiento informado: la exposición involuntaria de datos personales o la posibilidad de revictimización.

## Descubriendo la forense digital

La forense digital tradicional —también conocida como peritaje forense informática, ciberforense y peritaje forense de redes— suele definirse como la inspección científica de evidencias digitales recopiladas de dispositivos electrónicos, típicamente dividida por la National Institute of Standards and Technology (NIST) en **cinco fases: recuperación, conservación, análisis, interpretación y documentación**. Este proceso debe cumplir directrices legales estrictas, asegurando la integridad de las evidencias y su admisibilidad ante los tribunales.

A pesar de que la preocupación inicial de la sociedad civil por la forense digital estuvo motivada por casos de espionaje estatal, hoy estas **herramientas también son fundamentales para la investigación de otros tipos de amenazas digitales**. La forense digital se ha convertido en un instrumento clave en la defensa de los derechos humanos, especialmente frente a la expansión de la violencia digital Por lo tanto, se pueden adaptar sus prácticas a beneficio de organizaciones e individuos para quienes el espionaje estatal no necesariamente sea la única o principal amenaza.

En esta línea, la organización brasileña feminista MariLab, dedicada a promover la seguridad y el cuidado digital, detalla en su reciente informe "Forense Digital Feminista" otras formas de análisis forense digital:

1. Análisis forense para activistas, periodistas y/o personas defensoras de derechos humanos que buscan la justicia judicial para las violaciones de derechos humanos.
2. Investigaciones internas para organizaciones sin fines de lucro.
3. Investigaciones de violaciones de derechos humanos cuyo objetivo no es necesariamente la

2. Siglas en inglés para referirse a inteligencia de fuentes abiertas (*open source intelligence*) o información digital de fuentes abiertas (*digital open source information*).

judicialización sino la denuncia pública de las violaciones de derechos humanos.
4. Atención individualizada a víctimas de incidentes de seguridad digital.

Independientemente del tipo de amenaza digital, el proceso investigativo de la forense digital sigue un abordaje más o menos estructurado: 1) recolección y almacenamiento de la evidencia digital; 2) conexión de los ataques identificados y; 3) análisis utilizando técnicas *OSINT*.

**Desde el Equipo de Investigación de Política (EdIPo), realizamos este procedimiento de forma intuitiva y sin formación técnica especializada**, con la finalidad de colaborar en la causa judicial de la periodista Julia Mengolini. Luego descubrimos que era una práctica reconocida y que algunas organizaciones de la sociedad civil la venían desarrollando como forma de autodefensa digital. Algunos retos y limitaciones que encontramos en nuestra experiencia:

- La brecha técnica especializada: para que la prueba digital sea validada por la justicia, debe cumplir algunas reglas estrictas. En ese sentido, la participación —o al menos el asesoramiento— de un especialista en informática forense se vuelve indispensable.
- Información poco accesible o que no es fácil de aprender de forma autónoma. Existe un lenguaje aún limitante para los *no informáticos*.
- Falta de infraestructura y recursos materiales limitados.
- Falta de protocolos y manuales estandarizados desde el mismo sistema de justicia, lo cual impide conocer los criterios probatorios en la recolección de pruebas en redes sociales.
- Construir una perspectiva política y ética propia que trascienda las lógicas policiales y judiciales en las que la forense digital fue concebida.

## La importancia de la forense digital desde la sociedad civil

La adopción de **metodologías forenses por la sociedad civil constituye una forma de producir evidencia colectiva, colaborativa, ética e independiente**, ante tiempos judiciales que desarman la urgencia política del caso. Es una forma de resistencia y autodefensa ante la creciente concentración de información y capacidad de producción de evidencia en manos del Estado y las grandes corporaciones tecnológicas.

Ante la necesidad de recopilar evidencias en casos relacionados a violaciones a los derechos humanos facilitadas por la tecnología, diferentes organizaciones especialistas en seguridad digital como Amnesty Tech, Citizen Lab, SocialTIC y otras han impulsado prácticas llamadas: **forense digital consentida**. Bajo esta metodología la víctima o persona afectada de una violencia digital brinda su consentimiento informado para la práctica forense y se le garantiza el control de la investigación, incluso sin tener conocimientos técnicos especializados.

La incorporación de la práctica forense digital en la sociedad civil, activismo o militancia es un fenómeno relativamente reciente, por lo cual **no existen prácticas preestablecidas, sobre todo dada la diversidad que existen entre las organizaciones que aplican la metodología**. Existe una variedad práctica, flujos de trabajo y hasta diferencia en los objetivos, pero lo más importante es la mirada ética y política durante todo el proceso.

A partir de estas experiencias, nuestra apuesta se enfoca en intentar construir una metodología propia y colectiva que nos permita transitar **de una forense digital focalizada en especialistas técnicos a una apuesta colaborativa y multidisciplinaria**. Con el propósito de contribuir a esta apuesta, reconocemos una serie de retos y desafíos:

- Traducir los conocimientos técnicos y especializados a lenguajes más accesibles, pero sin perder la precisión y la construcción de un método objetivo.
- Necesidad de unificar, sistematizar y colectivizar los retos, desafíos y lecciones aprendidas de las principales organizaciones que trabajan en temas de seguridad digital y cuidados digitales, a fin de ir construyendo un lenguaje común y estandarizado.
- Adaptar herramientas de fuentes abiertas para análisis de redes sociales, frente a los altos costos de los softwares privativos de análisis de datos.
- Sostener una ética política propia que priorice la defensa de los derechos humanos, evitando replicar lógicas extractivas o de control.
- Producir conocimiento abierto y replicable que no sean propiedad de un solo grupo, sino que permitan fortalecer la construcción de una práctica forense colectiva.

### Repensando el rol del experto

La falta de especialistas con la pericia técnica y los conocimientos procedimentales requeridos son una gran problemática en los entornos de defensa de los derechos humanos. Por otro lado, existe la **necesidad de construir herramientas y metodologías propias para brindar respuestas rápidas y efectivas** en los procesos de denuncia que acompañamos.

En el plano legal, el **perito técnico suele ser un profesional acreditado y respaldado por la justicia**. Por ejemplo, en España, se puede contratar a peritos privados, siempre y cuando sean titulados y acreditados expertos en la materia. En Brasil, el perito oficial encargado de un caso es nombrado por el juez y debe ser examinador legal titulado. En nuestro país, un perito informático debe tener título profesional habilitante e inscribirse en el registro oficial de peritos/martilleros cuando se trata de participar como especialistas en causas de la justicia nacional o federal. Es decir, **la acreditación del profesional técnico depende del Estado**.

**A esto se suma la marcada masculinización de los espacios informáticos**, donde las mujeres y disidencias se enfrentan a modelos técnicos homogeneizados, que limitan las oportunidades de formación, profesionalización y especialización, así como la construcción de prácticas forense con enfoques feministas e interseccionales.

Frente a la necesidad de construir herramientas propias, organizaciones como Defensive Lab Agency, un pequeño colectivo de Francia dedicado al desarrollo de softwares abiertos, **creó herramientas tecnopolíticas que puedan ayudar a las organizaciones de la sociedad civil**. Uniendo recursos de fuente abierta, con nuevas funciones que antes solo se conseguían en herramientas patentadas de costes elevados, en el marco del proyecto PiRogue Tool Suite (PTS Project), elaboraron una plataforma para ofrecer herramientas asequibles y poderosas para el análisis forense digital como una forma de contribuir con las violaciones a los derechos humanos.

Sin embargo, a pesar de este tipo de iniciativas comunitarias, **la pericia forense digital sigue dependiendo de otros recursos de altos costos para análisis más profundos**. Aunado al hecho de que el sistema de justicia válida como estándar softwares que pertenecen a grandes empresas privadas.

Frente a esta situación, consideramos importante **apostar por la construcción del experto colectivo y ciudadano**. Una práctica que trasciende la lógica individual y especializada del perito acreditado y apuesta por formas multidisciplinarias de investigación y acompañamiento técnico, donde el intercambio de saberes sea la apuesta política que haga posible una construcción colectiva real. Desde EdIPo, tratamos de contribuir desde ese lugar: **la construcción de espacios multidisciplinarios que pongan**

**en común sus diferentes saberes y construyan una inteligencia colectiva**, con la finalidad de generar respuestas rápidas, éticas y eficientes frente al avance autoritario del poder político y las asimetrías de poder que existen en el terreno digital.

## 4.2 Desafíos en el ámbito jurídico

En el ámbito jurídico los desafíos, así como las oportunidades, son diversos. Siguiendo el trabajo de Julian Corti, la irrupción del mundo digital no sólo transformó los modos en que se ejerce la violencia, sino también las formas en que ésta puede o no ser acreditada. La expansión de lo digital como espacio social, político y económico plantea desafíos inéditos para el sistema de justicia, que sigue operando bajo lógicas y estructuras heredadas del paradigma analógico. En el marco de la *Ley Olimpia*, que reconoce la violencia digital como una forma específica de violencia de género, es imprescindible advertir que el reconocimiento normativo de un derecho resulta insuficiente si no se acompaña de capacidades efectivas para producir, resguardar y validar la evidencia —en este caso, digital— que permita garantizarlo. **La brecha entre la ley y su operatividad técnica se convierte así en un nuevo espacio de vulnerabilidad para las víctimas**.

El proceso judicial contemporáneo se enfrenta a una doble digitalización: la de los hechos y la de los procedimientos. Esta condición hace de lo digital no un mero soporte, sino el campo mismo de la acción y del conflicto. En ese contexto, la producción de evidencia (imágenes, mensajes, metadatos, interacciones en redes, trazas de dispositivos) constituye tanto una oportunidad como una trampa. Oportunidad, porque habilita nuevas vías para la reconstrucción de los hechos; trampa, porque su fragilidad, volatilidad y dependencia de infraestructura tecnológica privada pueden volver imposible su utilización válida en juicio. Esto implica una transformación profunda en la cultura jurídica: comprender que **el acceso a la verdad procesal está mediado por actores, tecnologías y estándares que no son neutros**.

La evidencia digital, entonces, no puede pensarse fuera de su ecosistema político-tecnológico. Su producción y su resguardo dependen de la capacidad del Estado, **o la sociedad civil**, de formar a sus operadores, de integrar equipos interdisciplinarios y de dotarlos de recursos materiales adecuados. Pero también, y sobre todo, de interpelar a las corporaciones tecnológicas que hoy controlan la infraestructura de comunicación y almacenamiento de datos. Los prestadores de bienes y servicios digitales deben asumir responsabilidades concretas frente a la justicia y frente a los derechos. Las garantías de privacidad y seguridad que protegen a los usuarios no pueden operar como un manto de impunidad que impida investigar delitos o violencias cometidas en el espacio digital. De allí la necesidad de **avanzar hacia acuerdos globales de cooperación y estándares compartidos que equilibren el derecho a la intimidad con el interés público en la persecución de la verdad y la justicia**.

### Falta de legislación en el país

La situación se agrava en el caso argentino, donde no existen mecanismos claros que regulen de manera sistemática la incorporación de la prueba digital como medio probatorio en los procesos penales, ni protocolos sobre técnicas de investigación digital. Según ODIA (2020), esta ausencia genera una tensión permanente entre la necesidad de adaptarse a los nuevos entornos delictivos y el respeto por el principio de legalidad penal, que exige que toda medida restrictiva de derechos esté prevista en la ley procesal.

En la práctica, esta **carencia deriva en un escenario de alta discrecionalidad judicial**, donde la validez de la evidencia digital depende menos de estándares objetivos que de la interpretación del juez interviniente, del prestigio del perito y, en no pocos casos, del interés político del expediente. A su vez, en Argentina no hay una cadena de custodia digital estandarizada, lo que debilita la fuerza probatoria de

capturas, resguardos web o pericias informáticas si no son incorporadas y certificadas por organismos oficiales.

Aquí hay un asunto nodal, en la medida en que el **sistema de justicia nacional e internacional termina por validar softwares privativos y altamente cuestionados**, como el *UFED* (por sus siglas en inglés, que significan "dispositivo de extracción forense universal") de la empresa privada *Cellebrite*. Esta funciona con un código cerrado que explota el teléfono de maneras no conocidas ni auditables, y sin embargo para el sistema judicial produce prueba válida. Otros softwares, más transparentes, pero menos conocidos, podrían en cambio considerarse de menor legitimidad para la elaboración de evidencia digital, aún si son de código abierto y por tanto auditables por cualquier otro experto.

A esta fragilidad estructural se suma **la inexistencia de una infraestructura pública para el resguardo de evidencia de violencia digital**. Al no existir una herramienta judicial donde se pueda guardar información de violencia digital, todo queda librado a la capacidad de la propia víctima para conservar pruebas y encontrar algún espacio donde alojarlas de manera segura, lo que traslada al plano individual una responsabilidad que debería ser institucional. Esta ausencia de dispositivos públicos de preservación produce un primer filtro de acceso a la justicia: **sólo quienes cuentan con conocimientos técnicos, acompañamiento especializado o recursos logran sostener una prueba mínimamente robusta**.

Asimismo, la falta de regulación clara impacta directamente en el modo en que se obtienen y preservan los datos: la información recolectada mediante *scraping*[3] o rastreos informáticos sólo puede adquirir valor probatorio si el magistrado decide convalidarla, aun cuando no existan previsiones explícitas en los códigos de procedimiento. En este contexto, **la prueba digital en Argentina se sostiene más en prácticas de hecho que en garantías de derecho**: sin criterios uniformes se consolida un escenario de incertidumbre jurídica estructural.

Por demás, **el pasaje al sistema acusatorio en el fuero federal**, que se posterga de forma sistemática hace ya varios años, anticipa una profunda transformación en la dinámica de los litigios en general, y en el manejo de la evidencia digital en particular. Al desplazarse el eje probatorio desde el expediente escrito hacia la oralidad, se espera un mayor protagonismo del experto como testigo que certifica y valida la prueba proveniente de fuentes abiertas. En este nuevo esquema, el valor ya no reside únicamente en el informe técnico incorporado al proceso, sino en la capacidad de quien lo produjo para explicarlo, defenderlo y someterlo a contradicción en audiencia. Este cambio abre oportunidades significativas para investigaciones basadas en fuentes abiertas y en técnicas de forense digital, que pueden ser expuestas de forma clara, directa y sencilla ante el juez. Al agilizarse los tiempos en la producción de prueba, podría también propiciar la intervención temprana de equipos especializados. No obstante, se trata de un sistema que incrementa la discrecionalidad de la fiscalía, la dependencia del prestigio del perito y la politización de las controversias técnicas, lo que exige una preparación más sólida en términos metodológicos, comunicacionales y estratégicos para este nuevo escenario de litigio.

### Ejemplos de avances legales en otras jurisdicciones

En paralelo, Europa avanza en la construcción de un marco regulatorio que busca equilibrar la transparencia, la rendición de cuentas y la protección de derechos en el ecosistema digital. El Reglamento de Servicios Digitales (*Digital Services Act, DSA*) constituye hoy el principal laboratorio normativo en ese sentido en occidente. El 2 de julio de 2025, la Comisión Europea adoptó la legislación delegada del Artículo 40(4) de la *DSA*, que regula el acceso a datos de las plataformas por parte de investigadores autorizados (*vetted researchers*). Este mecanismo intenta reducir la asimetría informativa entre

3. Proceso de extracción y recolección de información de sitios web a través de algún software automatizado.

los grandes intermediarios digitales y la comunidad investigadora, permitiendo estudiar los riesgos sistémicos que la propia *DSA* busca mitigar: desinformación, discursos de odio, violencia digital o manipulación algorítmica.

No obstante, el régimen presenta importantes limitaciones legales y estructurales. Por un lado, el acceso se restringe a investigaciones vinculadas a los "riesgos sistémicos" definidos en los artículos 34 y 35, lo que limita el universo de estudios posibles y genera tensiones interpretativas. Por otro lado, el sistema de autorización carece de parámetros uniformes, otorgando amplia discrecionalidad a las autoridades nacionales para habilitar o denegar solicitudes de acceso. Además, la ley permite a las plataformas rechazar pedidos si consideran que la información es accesible por otros medios, trasladando al investigador la carga de justificar la necesidad y proporcionalidad de su solicitud.

A nivel estructural, el reglamento impone requisitos técnicos y de seguridad que, aunque razonables desde la perspectiva de la protección de datos, afectan desproporcionadamente a las instituciones del sur global, que suelen carecer de los recursos necesarios para cumplirlos. Esto podría derivar en una dependencia estructural de centros europeos o norteamericanos, condicionando la autonomía investigativa y la producción de conocimiento situado.

Aun con esas tensiones, la legislación delegada del Artículo 40 constituye un punto de inflexión: **reconoce la función pública de la investigación como componente esencial del control democrático sobre las plataformas**. En la arquitectura de la *DSA*, la investigación aparece como un eslabón crítico que conecta la transparencia, la fiscalización ciudadana y la capacidad regulatoria. **Sin acceso a los datos, los Estados y la sociedad civil quedan a ciegas frente a los informes de riesgo de las plataformas, sin posibilidad real de auditar ni contrastar sus afirmaciones**.

El debate europeo tiene proyección global. Iniciativas análogas —como la *Online Safety Act* británica o el Proyecto de Ley 2630 en Brasil— comienzan a replicar cláusulas de acceso a datos y cooperación entre investigadores y plataformas. En todos los casos, se consolida una idea central: **sin evidencia independiente sobre el funcionamiento de los sistemas digitales, no hay posibilidad de rendición de cuentas tecnológica**. La convergencia entre investigación OSINT y marcos legales como la DSA abre así un nuevo horizonte: uno en el que la transparencia y la verificación pública se vuelven condiciones necesarias para la justicia en el entorno digital. El desafío no reside solo en crear nuevas leyes, sino en construir capacidades comunitarias para conocer, auditar y disputar el poder de las plataformas. Solo a partir de ese conocimiento colectivo podrá garantizarse que los derechos reconocidos en el plano normativo encuentren efectividad en el terreno de lo digital.

## 4.3 Desafíos en el ámbito político y ciudadano

Por último, en un tercer plano, resulta relevante ampliar los interrogantes. A continuación, planteamos algunos senderos para potenciar la capacidad colectiva de influencia de la comunidad organizada en torno a estos asuntos, en el ámbito político y ciudadano.

### Experticia colectiva

Como ya se señaló, el tratamiento de la evidencia digital plantea numerosos desafíos. El sistema judicial se enfocó mayormente en el peritaje forense de dispositivos, ya que a través de ellos se puede probar numerosos delitos. Sin embargo, la experiencia que surge del caso Mengolini pone el foco en **la necesidad de que dentro de la sociedad civil surjan voces expertas capaces de desarrollar un**

**análisis independiente de la información disponible en fuentes abiertas**, tanto la proveniente de redes sociales como la reconstruible por otros medios. Es decir, la comunidad no solo puede y debe poner límites a la vigilancia constante por medios digitales que los Estados llevan adelante, sino que tiene la oportunidad de desarrollar sus propios mecanismos de inteligibilidad y reconstrucción a través del análisis pormenorizado y cuidadoso de fuentes abiertas.

En ese mismo sentido argumenta el trabajo de Gillet y Fan, que también integra este dossier. A nivel internacional, menciona la importancia de que se establezcan parámetros claros, objetivos, justificados y no sesgados para que se incorporen a los procesos judiciales expertos en fuentes abiertas digitales de información. Advierten que hasta el momento este tipo de expertos no han realizado hallazgos críticos en el marco de la Corte Penal Internacional, que es en donde les interesa incidir. Advierten que debiera establecerse con claridad las metodologías adecuadas, con retroalimentación de control de calidad, transparentes, accesibles, replicables, revisadas por pares y con control de sesgos.

Ahora bien, consideramos que esto tiene impacto no solo dentro del ámbito judicial, sino que **puede constituir una innovación relevante en el ámbito de la discusión pública**. En la presente hora se expresa una tensión entre la sobreabundancia de información, la proliferación de noticias falsas y la puesta en cuestión de todas las tradicionales instituciones productoras de verdad y legitimidad: justicia, medios de comunicación, ciencia, universidad, etcétera. El alzamiento por parte de organizaciones comunitarias de una voz colectiva, capaz de integrar y analizar la información proveniente de fuentes digitales abiertas, podría resultar un aporte significativo al momento que vivimos. Se trataría de **una voz cuya legitimidad se funde en su capacidad para transmitir y hacer comprensible lo que hoy resulta caótico e inescrutable**, en su transparencia para mostrar los mecanismos que hacen posible tal interpretación y en la participación de una comunidad activa que respalde y controle la evidencia producida y los análisis realizados.

## Dependencia tecnológica y soberanía digital

A su vez, la posibilidad de acceder o no a evidencia digital depende, en gran medida, de decisiones empresariales tomadas en otras jurisdicciones, guiadas por intereses económicos y marcos regulatorios ajenos. Lo que aparece como un problema técnico —la falta de respuesta o de protocolos de colaboración— es, en realidad, la manifestación de una asimetría de poder estructural: los Estados carecen de control sobre la infraestructura donde se desarrollan buena parte de los vínculos sociales y políticos contemporáneos. Este tipo de situaciones pone en evidencia la d**imensión política de la dependencia tecnológica** que atraviesa hoy a los sistemas de justicia y de gobierno.

En la arquitectura de poder digital, el Estado no solo se enfrenta a limitaciones técnicas o procedimentales, sino que asume —de manera tácita— su subordinación frente a infraestructuras corporativas opacas. De allí la urgencia de dar pasos efectivos hacia una **soberanía tecnológica** que reequilibre esas relaciones.

No se trata sólo de regular a las plataformas o exigir cooperación, sino de desarrollar capacidades propias para producir, preservar y auditar evidencia digital. En ese sentido, la justicia podría tomar medidas tendientes a garantizar el cumplimiento de los pedidos de información requeridos por el sistema argentino (tal como lo hizo el Tribunal Superior de Justicia de Brasil) y el congreso podría sancionar normativas para que las plataformas adapten sus propios términos a protocolos que permitan el cumplimiento de las leyes locales (tal como lo realizó la Unión Europea).

Por demás, aún si se avanzara en esos sentidos y se lograra un mínimo control democrático del funcionamiento de las plataformas en territorio nacional, **queda pendiente la necesidad de desarrollar infraestructuras tecnológicas colectivas, guiadas por criterios alternativos a la captura de la**

**atención y su monetización**. Infraestructuras de uso público, que pueden estar sostenidas en iniciativas estatales en torno al bien común o en iniciativas colectivas y distribuidas, retomando el espíritu del internet de inicios de siglo. Algo de esto último pervive hoy en Wikipedia, pero fuera de esa experiencia no abundan ejemplos de iniciativas similares. **Mientras la mayor parte de la vida digital transcurra en plataformas corporativas, la posibilidad de una escena pública y democrática parece una quimera**.

### Litigio como arena estratégica de disputa

Por último, es preciso reflexionar que las **transformaciones necesarias, generalmente, no surgen de cambios graduales y progresivos**, sino que son la resultante de procesos complejos y conflictivos. En ese sentido, casos como el de Julia Mengolini muestran la potencia de las historias singulares, donde se anudan violencia y resistencia, para escenificar y problematizar un conjunto de cuestiones estratégicas y urgentes para el presente. Son historias donde aparece la impunidad, pero también se la enfrenta. **El litigio estratégico es una vía con que la ciudadanía cuenta para contribuir a torcer el rumbo y escribir nuevas historias**, no solo en el marco de los procesos judiciales, sino también más allá de ellos. En ese sentido, es preciso pensar en los antagonismos estratégicos como un medio para potenciar la capacidad colectiva de resistencia y acción. No se trata de un camino sencillo, sino de experiencias que contribuyan a movilizar alianzas duraderas y alimentar un horizonte para la vida en común.

## 5. Cierre

El caso de Julia Mengolini expone con claridad cómo las violencias digitales ya no pueden pensarse como hechos aislados ni meramente simbólicos, sino como prácticas organizadas, con participación de actores estatales y paraestatales, capaces de producir daños reales en la vida, la salud y la integridad de las personas. A lo largo del texto se evidenció que estas violencias se sostienen en un entramado de impunidad estructural, alimentado por la opacidad de las plataformas, la fragilidad de los marcos normativos y las limitaciones técnicas del sistema judicial. Al mismo tiempo, el trabajo muestra que la producción de evidencia digital, mediante metodologías *OSINT*, análisis de redes y prácticas de forense digital desde la sociedad civil, constituye hoy una herramienta indispensable para combatir esa impunidad.

Sin embargo, la experiencia también deja lecciones que trascienden el caso puntual: sin infraestructura pública para preservar pruebas, sin legislación específica, sin cooperación efectiva de las plataformas y sin capacidades técnicas estatales fortalecidas, el acceso a la justicia frente a la violencia digital seguirá siendo desigual. En este escenario, el litigio estratégico, la construcción de experticia colectiva y la disputa por la soberanía tecnológica aparecen como arenas fundamentales de intervención democrática. El desafío no es solo técnico o jurídico, sino profundamente político: garantizar que el espacio digital no se consolide como un territorio de disciplinamiento, censura y violencia legitimada desde el poder, sino como un ámbito donde los derechos puedan ser efectivamente ejercidos y defendidos.

# Enfoques, estrategias y dificultades en el litigio de agresiones por parte de milicias digitales de ultraderecha

Annick Aubert y Camila Palacin, integrantes de Argentina Humana

## 1. Introducción

El presente informe parte del intento de comprender cómo se le puede hacer frente a las nuevas formas de violencia que proliferan en el mundo y en particular en la Argentina, específicamente desde la pandemia del COVID.

Nace de la inquietud de ordenar lo que en los hechos venimos trabajando desde hace un tiempo: ¿Cuáles son las prácticas violentas que se reproducen a través de las redes sociales? ¿Cómo trascienden a la vida material? ¿Qué herramientas tenemos para paliarlas? ¿Qué nos falta?

En este Informe vamos a sistematizar a partir de distintas estrategias de investigación desplegadas (entrevistas a víctimas, a usuarios, a informantes clave, mapa de redes) algunas de las diferentes formas de violencia digital que existen en el mundo: *doxeo, swatting, violencia sexual, slapp y review bombing*. También a través del análisis de casos que estuvimos abordando judicialmente queremos analizar cómo se reproducen estas violencias en la Argentina, particularmente las que tienen origen ideológico, pensando a su vez las herramientas legales con las que contamos para afrontarlas. Presentaremos cuáles fueron los hallazgos concretos que surgieron a partir de estos casos y al reflexionar acerca de los problemas y avances con los que nos encontramos, intentaremos aproximarnos a una conclusión con algunas propuestas sobre la materia.

## 2. Metodología y estrategias de abordaje

A partir de la asunción del gobierno de Javier Milei en Argentina tuvimos la fuerte sospecha de que la violencia digital que venía en aumento se instauraría como una metodología militante del gobierno actual.

Como consecuencia de esto decidimos elaborar una serie de estrategias para comprender estas nuevas formas de hacer política a través del intento de silenciamiento de quienes se presentan como opositores. Entendimos que esta no era solo una expresión local, sino que también venía expandiéndose alrededor del mundo pero nos resultó fundamental poder pensar maneras de enfrentarlas.

Una de las primeras estrategias utilizadas para poder echar luz sobre este fenómeno y también poder al mismo tiempo intervenir, fue armar un mail al que las personas podían contactarse con nosotros -abogados y militantes políticos- para contarnos situaciones de violencia política que estuvieran viviendo y evaluar, en caso de ser posible, cómo intervenir. En ese proceso se buscaba además de brindar herramientas, construir un receptor que acreditara que aquello que pasaba en las redes sociales, efectivamente era violencia. De modo simultáneo a la recepción de denuncias llevamos a cabo un análisis de los intercambios en redes sociales, en particular de "X", enfocándonos en aquellos en donde podíamos reconocer alguna situación de violencia.

A su vez, se realizaron entrevistas a las víctimas de estas violencias y a informantes clave que permitieron acceder a conocimiento específico sobre el funcionamiento y lógica de las redes en general y de "X" en particular. Estas entrevistas también nos permitieron ir construyendo un modelo de red, identificando nodos (personas humanas, jurídicas, usuarios de "X", etc.) y vínculos entre estos nodos (laborales, gubernamentales, afectivos, etc.) Este modelo resulta más que pertinente para entender el modo en el que se relacionan los distintos usuarios en las redes sociales y por ende, comprender cuáles son aquellos que tienen un rol preponderante. A su vez, este sistema nos está permitiendo empezar a comprender mejor los vínculos entre distintas dependencias gubernamentales y las violencias desplegadas.

# 3. La violencia digital y sus modalidades

## Doxeo

Uno de los tipos de violencia digital más ejecutados en el último tiempo, especialmente por los grupos de derecha, consiste en el *doxeo*. Esta nueva forma de hostigamiento digital implica compartir en internet (generalmente en X) datos personales como números de teléfono, domicilios personales y laborales con imágenes de los mismos, documentos de identidad, situaciones crediticias, datos de lugares de trabajo, entre otros con el objetivo de que los demás usuarios tengan la posibilidad de amenazar u hostigar a la persona *doxeada*. Si bien se trata de una práctica que adquiere cada día más fuerza, no existen en el mundo muchos avances en el plano legal para sancionarla.

En Hong Kong se aprobó en octubre del 2021 una Ordenanza sobre datos personales[1] que creó dos nuevos delitos para castigar el *doxeo*. En uno de ellos contempla una pena atenuada para quien revele cualquier dato personal de alguien sin su consentimiento con intención de provocar un daño o con mera imprudencia. El otro delito está pensado para quien revela los datos, con intención o imprudencia y esta revelación produce un daño concreto para la persona o su familia.

## Swatting

Una vez filtrados los datos y disponibles en la red se inicia un segundo momento en el que la violencia

1 https://www.pcpd.org.hk/english/data_privacy_law/amendments_2021/amendment_2021.html

trasciende la pantalla para llevar el hostigamiento mencionado en el apartado anterior a otro nivel a través de lo que se conoce como *swatting*.

El término proviene de los Estados Unidos y cobró una progresiva relevancia desde el año 2008. Debe su nombre a que inicialmente el *swatting* se utilizaba para movilizar a los servicios de emergencia dando aviso de un hecho grave y generando así un fuerte operativo del SWAT (Special Weapons And Tactics). Esta modalidad se hizo popular en el mundo de los videojuegos donde realizaban llamadas en las que decían la dirección de quien estaba transmitiendo por *streaming*. Un caso popular ocurrió durante la transmisión de una partida del videojuego *Counter-Strike* donde el streamer fue irrumpido por la policía e inmovilizado debido a los llamados de alguien que estaba viendo el vivo de *streaming*. El operativo fue visto en directo por más de mil personas, siendo luego replicado en YouTube más de 4 millones de veces, volviendo al *swatting* una "broma de moda" entre los jugadores de videojuegos[2].

Dentro de ese universo *gamer*, el *swatting* comenzó a utilizarse para atacar a las mujeres de la industria. El movimiento "GamerGate", un movimiento de derecha en contra del "feminismo, diversidad y progresismo en la cultura de los videojuegos"[3] utilizó contra sus víctimas tanto técnicas de *doxeo* como de *swatting*.

En Estados Unidos los casos de *swatting* fueron encuadrados legalmente, dependiendo los casos, en las leyes federales de información falsa y engaños, *stalking*, amenazas y fraude electrónico. Algunos estados incorporaron leyes de manera puntual, por ejemplo en California quienes ejecutan el *swatting* tienen que luego hacerse cargo del costo del operativo que fue desplegado sin motivación real y, tanto California como Nueva Jersey, encuadran las denuncias falsas en delitos de odio cuando están motivados por algún tipo de discriminación[4].

## Filtración de contenido íntimo[5]

Este es un tipo de violencia ejercido cuando las víctimas son mujeres o disidencias sexuales, siendo una práctica que sucede no sólo por causas políticas o ideológicas, sino que se encuentra muy difundida en la web como forma de violencia contra las mujeres.

Se trata de difundir contenido íntimo o sexual de personas mayores de edad sin su consentimiento. El contenido puede haber sido obtenido a sabiendas de la persona (cuando ella se lo envía a quien luego lo difunde) o sin conocimiento (cuando se obtiene como consecuencia de un hackeo o desconociendo la mujer que estaba siendo filmada o fotografiada).

Este delito suele ser iniciado por una persona pero luego adquiere varios autores dado que el contenido es replicado reiteradas veces por otras personas en la web.

Actualmente la OEA se encuentra en proceso de elaborar una Ley Modelo para prevenir, sancionar y erradicar la violencia contra las mujeres en entornos digitales con el objetivo de que sirva de guía para adecuar la legislación y desarrollar planes nacionales y políticas públicas en la materia[6].

---

2 https://www.levelup.com/noticias/287257/Policia-interrumpe-stream-de-CounterStrike/pagina/1

3 https://en.wikipedia.org/wiki/Gamergate_(harassment_campaign)

4 https://www.nolo.com/legal-encyclopedia/the-crime-of-swatting-laws-and-penalties.html

5 Recomendamos para ahondar este tema el libro. "Violencia de género digital" de Zerda María Florencia. (2024). Hammurabi, 2024.

6 https://www.diariojudicial.com/news-99263-en-la-busqueda-de-un-limite-a-la-violencia-digital

Ya son varios los países que cuentan en su legislación con normas que castigan la difusión no consentida de contenido sexual como Japón, Portugal, Filipinas, Alemania, España, Canadá, México, Brasil y algunos estados de EEUU, entre otros.

No en todos los países se encuentra tipificado penalmente y considerado un delito. En algunos se impone simplemente una multa. En Israel, por ejemplo, quienes difunden material íntimo es considerado como agresor sexual, siendo sancionados con penas de hasta cinco años de prisión[7].

## SLAPP (Strategic Lawsuits Against Public Participation)

La metodología del *SLAPP*, referidas sus siglas a la estrategia de iniciar demandas contra la participación u opinión pública, tiene como objetivo silenciar a periodistas, organizaciones sociales y figuras públicas agotando a los demandados con largos procesos judiciales.

En Estados Unidos y Canadá se han promulgado leyes AntiSLAPP que permiten a los tribunales evaluar si una demanda es contra una actividad de interés público, examinar si efectivamente hay pruebas y revisar si el caso tiene expectativas de éxito. Estas leyes brindan procedimientos para poder desestimar casos de manera temprana cuando estos afecten asuntos de interés público, evitando así el efecto amedrentador que persiguen los casos de *SLAPP*.

La Corte Interamericana reconoció explícitamente el término *SLAPP* como un peligro para los Derechos Humanos y libertad de expresión en el caso "Palacio Urrutia y otros c. Ecuador[8]". En este caso, el entonces presidente de Ecuador denunció penalmente a un medio de comunicación y a diversos periodistas por determinados dichos públicos y la CIDH definió el concepto *SLAPP* y concluyó en que es un ejercicio abusivo de los mecanismos judiciales. De esta manera, impulsó a que los Estados adopten medidas concretas para frenarlo. Determinó que en estos casos se acude a la vía judicial *"no con el objetivo de obtener una rectificación sino para acallar las críticas que se formulan sobre su actuación en el ámbito público"*.

En este mismo fallo, se mencionan a las leyes de Ontario como un ejemplo contra el *SLAPP*. Haciendo mención al establecimiento de mecanismos que permiten desechar las demandas cuando se advierta que limitan el ejercicio de la libertad de expresión sobre casos de interés público.

También existen diversos fallos de tribunales superiores contra el *SLAPP* pero principalmente de casos donde quien denuncia es el Estado o un funcionario público a un medio o un periodista. Lo que notamos, en línea con lo señalado por la Global Freedom of Expression de la Universidad de Columbia es que, por un lado, *"los tribunales inferiores no están aplicando correctamente las normas internacionales en materia de libertad de expresión en sus casos"* (GFoe, 2024, p.30) lo que genera que estas decisiones vengan después de años y gastos de litigio. Además, parece no existir jurisprudencia en relación a casos de privados contra otros particulares.[9]

---

7 http://www.timesofisrael.com/israeli-law-labels-revenge-porn-a-sex-crime

8 Global Freedom of Expression | Palacio Urrutia v. Ecuador - Global Freedom of Expression

9 Para profundizar sobre este tema, recomendamos la lectura del paper de la Global Freedom of Expression de la Universidad de Columbia titulado " ¿Cómo responden los tribunales a las SLAPP? Análisis de decisiones judiciales seleccionadas de todo el mundo". https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2023/08/GFoE_%C2%_BFCo%CC%81mo-responden-los-tribunales-a-los-SLAPP__PAPER-1.pdf

## Bombardeo de reseñas (review bombing)

El bombardeo de reseñas es el nombre que lleva la práctica de reseñar negativamente de forma masiva algún tipo de producto, servicio o lugar con el fin de influir en su popularidad o en sus ventas. Mediante este método se publican calificaciones o comentarios que intentan alterar la percepción de los posibles consumidores respecto a lo que se ofrece.

Es un método muy utilizado en las plataformas que califican videojuegos, películas o series y también en Google Maps en las reseñas que se pueden dejar de los diferentes lugares o comercios.

En Estados Unidos la Comisión Federal de Comercio implementó una serie de reglas que buscan frenar la manipulación de reseñas falsas ya sea de usuarios que no existen (bots o generadas por la IA) o que no han tenido efectivamente experiencia con el producto o servicio. Se prohíbe también que las empresas compren o creen reseñas falsas y aquellos que las compren y/o las difundan de manera consciente estarán sujetos a sanciones civiles. Esta medida busca que los usuarios puedan reportar cuando ven una reseña sospechosa y en caso de ser así, la Comisión puede establecer sanciones económicas a los individuos o las empresas que infrinjan lo establecido.

# 4. Análisis de casos

A continuación expondremos algunos de los hechos concretos vinculados con diferentes figuras delictivas que nacen o se relacionan con la digitalidad que llevamos al ámbito judicial contando sus avances y/o resultados:

## Violencia digital por difusión de imágenes íntimas

### a. Caso Lucila De Ponti

**Qué pasó:**
Lucila de Ponti es una política de Santa Fe que ejerció como diputada nacional entre 2015 y 2019 y, actualmente, se desempeña como legisladora provincial. En el año 2017 en la red social "Twitter" y en diversos portales de internet publicaron fotos íntimas de ella obtenidas de manera ilícita.

Días después de la presentación de las listas electorales para competir en las elecciones Primarias, Abiertas, Simultáneas y Obligatorias (PASO), que se desarrollarían en agosto del 2017 y en las cuales Lucila iba de candidata, le comenzaron a llegar unos mails en los que le advertían de una actividad irregular en su cuenta personal de correo. A raíz de ello tuvo que cambiar la cuenta en varias oportunidades. Habían dos correos electrónicos que le llamaron la atención porque no provenían de la cuenta de correo que Google utiliza oficialmente para notificar este tipo de situaciones, sino de "nuevasesioninicio@gmail.com", pero ambos parecían ser del soporte técnico oficial de Google-Gmail y la alertaban de la actividad irregular en su cuenta. Estos correos contenían un enlace a fines de que pueda restablecer su contraseña, lo que creía haber realizado.

Luego de esto, el 3 de julio del 2017, comenzó a circular en la red social de "Twitter" y luego en diferentes portales, una fotografía de ella sin ropa que fue robada de la nube de fotos de Google.

A partir de este hecho Lucila efectuó la denuncia correspondiente ante la UFEM Unidad Fiscal Especializada en Violencia contra las Mujeres del Ministerio Público Fiscal de la Nación y la UFECI (Unidad Fiscal Especializada en Ciberdelincuencia).

**Qué se hizo:**
Se le envió a Google un Oficio judicial solicitando que aporte "la totalidad de direcciones de IP utilizadas para acceder a la cuenta durante el período comprendido entre los días 22 de marzo de 2017 y 3 de julio de 2017 –ambos inclusive-, con indicación de fecha, hora y zona horaria de la conexión; como así todos los datos (correo alternativo, teléfono de verificación, servicios asociados) relativos a dicha cuenta que hayan sido agregados y/o modificados" y la información del mail mediante el cual la contactaron haciéndose pasar por cuentas oficiales de la empresa.

También se les pidió a AMX Argentina SA (Claro) y a Telecom Personal SA que brindaran toda la información que tuvieran vinculada a los diferentes números telefónicos que eran partícipes del hecho delictivo.

Con los datos aportados por las empresas se logró identificar a dos sujetos, los cuales fueron investigados por la policía y debidamente allanados, habiendo secuestrado en sus domicilios diversos objetos (computadoras, teléfonos celular, chips) que fueron claves para determinar su participación en el hecho.

Además el juzgado le ordenó a varias plataformas virtuales y medios de comunicación que eliminen de sus portales las fotografías de carácter privado e íntimas de la Diputada Lucila María De Ponti.

Ante la justicia civil se presentó un amparo con una medida cautelar para instar, tanto a las redes sociales como a los medios de comunicación donde se estaban difundiendo las fotos íntimas, a que den de baja los usuarios que lo hacían y cesen las noticias dañosas.

De esta forma, el Juzgado Nacional en lo Civil interviniente dictó una medida en la que ordenó a diferentes empresas de comunicación como también a redes sociales (Google, Yahoo, Instagram, Facebook, Twitter) la inmediata eliminación y retiro de sus portales, redes sociales y medios de difusión de todo contenido vinculado a la denunciante.

Sin embargo, la empresa Twitter (hoy en día "X") nunca pudo ser notificada. Desde la propia justicia le comunicaron a Lucila que nunca habían tenido buen resultado intentando notificar a esta red social y que el único precedente que existía en la materia era el de un caso en el que la modelo Victoria Vanucci demandó a Twitter por la difusión de fotos que, según ella, la agraviaban. En aquella causa la justicia falló en contra de Twitter en primera instancia y los obligó a que eliminaran todos los dichos y fotos en donde se dirigieran a Vanucci de manera gravosa.[10] Sin embargo, **para intentar notificar a Twitter de esta sentencia la mediática tuvo que ir hasta el lugar donde la empresa del pajarito tenía la sede central: Dublín, Irlanda.**

Debido a este antecedente, **Lucila emprendió un viaje fugaz al país europeo con el fin de intentar que Twitter se notificara**. Era complejo, no solamente porque debía sacar el

10 https://www.infobae.com/teleshow/infoshow/2016/12/28/la-justicia-le-ordeno-a-twitter-eliminar-los-mensajes-que- ofendan-a-victoria-vannucci/

pasaje para ir, sino también porque había ciertos requisitos que cumplir para poder intentar el cometido: como llevar una carta específica firmada por el consulado argentino. Gracias a la ayuda que recibió, logró conseguir los papeles necesarios para viajar. Pero al llegar, **pese a su insistencia, nadie quiso recibir la notificación**. Terminó dejándola en el consulado argentino en Irlanda pero sin lograr el objetivo buscado.

En una charla con ella para armar este informe nos contó que **la forma en la que lograron que en Twitter se bajaran las publicaciones de quienes difundían las imágenes íntimas fue con la organización de sus conocidos** que, apenas veían una publicación con las fotos, comenzaban a denunciar masivamente hasta lograr que la desactiven.

**Cómo concluyó:**
La justicia penal federal de Rosario en el 2023, es decir seis años después del inicio de la causa, condenó a los dos imputados en el caso de Lucila a la pena de tres años de prisión de ejecución condicional por los delitos de amenazas coactivas en concurso ideal con los delitos de acceso ilegítimo a un sistema informático y falsificación; uso de una marca registrada y extorsión en grado de tentativa.

En la causa civil la justicia ordenó el cese de las fotos en los medios de comunicación ya que tenían domicilios en el país y acataban las normas y sentencias judiciales. Sin embargo, como se contó en el punto anterior, no corrió con la misma suerte en relación a las redes sociales, específicamente Twitter. Al no poder notificar, la red social no tuvo la obligación de hacerse cargo del comportamiento delictivo de sus usuarios y lo único que les quedó fue organizarse colectivamente para denunciar y esperar que, eventualmente, se bajaran las fotos.

# Amenazas por redes sociales

## b. Caso Ofelia

**Qué pasó:**
Ofelia Fernández es una referenta política que fue legisladora por la Ciudad de Buenos Aires entre el año 2019 y 2023.

El día 15 de julio de 2020 Ofelia realizó una denuncia ante la UFECI (Unidad Fiscal Especializada en Ciberdelincuencia) por una publicación efectuada a través de la red social Twitter (actualmente X) por parte de usuarios que le dijeron cosas como: "DATE UNA VUELTA POR LA MARCHA, GORDA, ASI TE SUBIMOS AL FALCON, PAJERA", "Acá les muestro mi falcon, lo armé de cero y me da bronca que @OfeFernandez_ me niegue una vueltita" y "PERO QUE TIENE DE MALO? TE INVITÓ A DAR UNA VUELTA EN AUTO. YO SOY MAS GALÁN Y TE LLEVO A DAR UNA VUELTA EN HELICÓPTERO SOBRE EL RÍO DE LA PLATA."

Así se logró obtener la información de los usuarios como los correos electrónicos, creación de IP, conexiones de IP, teléfono, y demás.

También se le pidió a la empresa "Mercado Pago" que informara sobre un abonado que había surgido de la investigación y así se dio con el nombre del usuario a partir de lo cual se pudo conseguir mayor información (número de teléfono, nombre de dos personas abonadas vinculadas a esa cuenta, y el historial de la conexión del IP.) A través de la IP de donde se creó la cuenta se determinó que pertenecía a un cliente de la firma de Telecom con domicilio

en la provincia de Córdoba, dato que después se confirmó con otras informaciones.

El imputado fue llamado a indagatoria, donde reconoció lo que había dicho y declaró estar arrepentido: "estoy totalmente arrepentido de haberlo hecho y cuando lo hice era muy joven, tenía 19 años". Añadió que no fue su intención que se sintiera amenazada: "No fui consciente de lo que podía un comentario de esta índole hacer en la persona".

**Qué se hizo:**
En principio la Fiscalía actuante pidió el archivo y por eso Ofelia tuvo que constituirse como querellante para continuar con la acción e instar el proceso ella.

A través de la UFECI se obtuvieron capturas de los mensajes amenazantes que habían sido borrados.

Luego, se verificaron los usuarios y perfiles de las cuentas denunciadas. Para ello se solicitó a la División Investigaciones Especiales de la Policía de la Ciudad una búsqueda de los usuarios denunciados en fuentes abiertas de información para esclarecer la identidad de los usuarios, y conforme las medidas propuestas por la querella, se solicitó colaboración al Departamento de Justicia de los Estados Unidos de América para que por su intermedio se requiera a la empresa Twitter, radicada en ese país, la información básica de los usuarios que efectuaron los dichos gravosos.

Así se efectuó un allanamiento en el domicilio identificado, vía exhorto y con intervención de la División Investigaciones Especiales donde se encontraron diferentes dispositivos electrónicos, los cuales fueron secuestrados.

**Cómo concluyó:**
El imputado fue procesado como autor del delito de amenazas coactivas agravadas, en concurso ideal con el delito de incitación al odio y a la violencia y con un embargo sobre sus bienes de cinco millones de pesos. Actualmente la causa fue elevada a juicio aunque se discute si la competencia es de la justicia Federal o Nacional.

## c. Caso Juan Grabois

**Qué pasó:**
Marco Antonio Chediek el 22 de noviembre de 2023 publicó un video en su cuenta personal de la red social "Tik Tok" en donde manifestaba"... Juan Grabois tené cuidado con los milicos, no tenemos nada que perder, fíjate lo que le paso a Morales, a vos en la 9 de julio te tenemos regalado..." y también que "utilice chaleco porque no va a ver balas de gomas, sino que van a ver balas de verdad".

Con esto, Chediek buscaba amenazar dirigentes sociales para que no realicen ningún tipo de movilización social en los espacios públicos y bajo consignas que constituyan reclamos contra el futuro gobierno, ya que la misma traería consecuencias para con sus seguidores. En el mismo video el denunciado incita públicamente a la violencia colectiva contra un grupo de personas determinado en función de supuestas afinidades políticas, contrarias a las suyas.

A raíz de esto, Grabios efectuó una denuncia en la justicia penal federal por el delito de amenazas coactivas.

**Qué se hizo:**
Como primeras medidas de investigación el Juzgado actuante, entre otras cuestiones, pidió la intervención de la División Investigación de Amenazas e Intimidaciones Públicas de la PFA para que arbitre medidas necesarias con el fin de verificar los datos personales de la cuenta de Tik Tok de Marcos Antonio Chediek (@marco.chediek) para así determinar si se encontraba vinculado a actividades que podrían poner en riesgo al denunciado o a otros dirigentes sociales.

**Cómo concluyó:**
Poco más de un mes de iniciada la causa, luego de la declaración indagatoria, Chediek fue procesado por el delito de amenazas en concurso ideal con el delito de incitación a la violencia colectiva y se le trabó embargo por $600.000 (seiscientos mil pesos). De esta manera, la causa se elevó a juicio encontrándonos a la espera de su desarrollo.

## d. Caso Nati Zaracho

Los días 10, 20, 21 y 22 de enero del 2024 la referenta del Frente Patria Grande y diputada nacional Natalia Zaracho recibió en su cuenta de Facebook mensajes en los que le decían cosas como "te vamos a matar puta traidora", "estás en un lugar que no te corresponde por bestia" y "no vas a durar mucho" enviados de dos perfiles distintos. A raíz de esto realizó una denuncia por amenazas coactivas ante la justicia federal.

**Qué se hizo:**
En un primer lugar la fiscalía interviniente logró determinar a través de los nombres de los usuarios los números de identidad y domicilios fiscales, valiéndose de informes NOSIS y del Registro Nacional de las Personas. Las fotografías del RENAPER coincidían con las de los usuarios de Facebook que habían amenazado a Natalia.

Además, y como prueba más relevante, **se le envió Oficio a Meta Platforms Inc. con sede en California, Estados Unidos**, con el objetivo de que informe respecto a los dos usuarios investigados: nombres y apellidos, día, hora e IP de creación, correo electrónico de registro y alternativo teléfono de verificación, servicios asociados, etc.); y detalle las direcciones de IP utilizadas para acceder a tales cuentas desde el 1° de enero de 2024 hasta la actualidad, con indicación de fecha, hora y zona horaria de la conexión.

Esto fue respondido por la empresa estadounidense, pudiendo determinar los correos electrónicos asociados a las cuentas, los números de teléfono de los usuarios y las direcciones de IP mediante las cuales se accedió a la cuenta -logs de conexión. Así, mediante oficio a Telecom S.A. pidiendo información de los abonados telefónicos, se verificó que los números pertenecían efectivamente los usuarios que le mandaron los mensajes amenazantes. También, mediante las IP se logró determinar los domicilios de los titulares.

**Cómo concluyó:**
Se suspendió el juicio a prueba y los acusados tuvieron que cumplir con medidas impuestas por probation.

# Doxeo y swatting:

## e. Caso A

**Qué pasó:**
A es una joven que se define como nacional y popular en la red social X. Aquí suele organizar *spaces* -espacios virtuales de la red social donde la gente puede conversar a través de audio en directo- en los que cualquiera puede participar. Allí empezaron a sumarse algunos usuarios que, con el tiempo se enteró, pertenecían a un grupo autodenominado "KFC" (kiosco, falopa y coquita). A veces entraba uno, a veces dos, a veces tres. Trolleaban, molestaban y atacaban. Eran libertarios, supo decir, pero se comportaban como nazis. Ella, feminista y peronista, se hartó y los bloqueó. En ese momento, KFC comenzó su represalia.

El grupo la apodó "la lechoncita" y subió a su sitio web (https://kfcok.net/) un informe crediticio que incluía su dirección. También filtraron su número de teléfono, una foto de la puerta de la casa y datos de sus cuentas bancarias.

Días después, un hombre muy grandote "con pinta de patovica" se apersonó en la entrada de su casa. La madre estaba barriendo la vereda. Él la puso contra la pared y la amenazó: le dijo que si la puta de su hija no se callaba la boca los iba "a matar a todos". Mencionó el nombre de su padre, del hermano y del sobrino.

A partir de ese momento comenzaron a suceder diversos ataques en su domicilio. Este grupo (KFC) anunció en Marketplace que se regalaba una heladera y otros objetos en su domicilio, por lo que acudieron varias personas. También se pelearon adrede con gente en las redes sociales, a quienes le pasaron la dirección de su domicilio diciéndoles "vení a buscarme acá, cagón". Lo que ocasionó que una persona terminara tirándole piedras a la puerta y a las cámaras de seguridad que instaló la familia de A luego del primer incidente.

La obsesión misógina que tienen con A generó que le dedicaran varios espacios de Twitter del grupo "KFC" de forma casi exclusiva. Organizaron un *space* titulado "paja grupal escuchando la voz de A". Luego le enviaron el video de un hombre masturbándose mientras sonaba la voz de ella.

Después de aquello mandaron a colgar un pasacalles en la esquina de su casa que decía: "Nos encanta tu voz" (firma: KFC). Acá es cuando procedió a llamar a la policía y se inició una denuncia que recayó en la Provincia de Buenos Aires, donde se encuentra su domicilio.

En un *space* llamado "Gauchito Gil", planificaron instalar una estatua del santo popular en la entrada de su casa con el objetivo de llenar la puerta "de villeros" que peregrinaran hacia allí. Finalmente, contrataron a alguien que la colocara, tal como lo registran las cámaras de seguridad, pero no tuvo el efecto social esperado.

**Qué se hizo:**
Cuando le instalaron el pasacalle con la frase "nos encanta tu voz" en alusión a los videos donde se masturbaban con la voz de esta joven de fondo, se inició una denuncia que empezó su trámite en la justicia local de la Provincia de Buenos Aires, específicamente en La Matanza.

En primer lugar la persona contratada para colocar el pasacalles declaró ante la policía. En aquel acto aportó información de quiénes lo contrataron y efectuaron el pago. Así la justicia

pudo averiguar que la operación se hizo a través de la plataforma Mercado Libre con un usuario a nombre de la "Asociación Civil de los Consumidores por la Libertad" y con un número de teléfono asociado.

Este dato fue clave para poder dar con personas físicas y lograr salir de la esfera de X que, como se explicará después, es un obstáculo concreto para las investigaciones judiciales.

Con la intervención del Departamento de Ciberdelitos del Ministerio de Seguridad de la Provincia de Buenos Aires comenzó una investigación en la cual se logró dar con las personas titulares, los datos de identificación de aquellos y los de la Asociación a través de la IGJ.
A través de la información brindada por Claro SA se pudo saber que el número vinculado a la cuenta de Mercado libre estaba a nombre de Federico Gorga.

Se realizaron tareas de investigación en los domicilios de la Asociación Civil de los Consumidores de la Libertad pero al no identificarse actividades relacionadas con estas personas ni tampoco ellos mismos, no se llevó a cabo ningún allanamiento.

Por último, intentamos en reiteradas oportunidades, mediante oficio judicial a San Francisco, Estados Unidos, solicitar a la red social X información de por lo menos cuatro cuentas que son las que hostigan a la denunciante constantemente y que propagan las situaciones de acoso en su hogar y en las redes.

Sin embargo X no contestó y al día de hoy la causa se encuentra estancada en la investigación por este motivo.

**Cómo concluyó:**
Al no tener contestación de X y no poder recabar más datos por fuera de esa red que no fueran los que ya se investigaron, la causa quedó inmovilizada. Este freno
dio cuenta, una vez más, que la justicia no cuenta con herramientas idóneas para investigar este tipo de hechos.
La falta de avances judiciales llevó a un desgaste por parte de la denunciante lo que se vio traducido en la imposibilidad, por diversas razones, para continuar con el proceso.
Si bien no conseguimos frenar los ataques por la vía judicial, lo que KFC pareciera buscar, esto es el silenciamiento de sus víctimas, no tuvo un final exitoso. El grupo no pudo con el objetivo de que la joven se vaya de X y deje de armar spaces de discusión política. Actualmente, aún sin la continuidad de la causa, A sigue en la red social participando y opinando de manera activa, no habiendo podido KFC doblegarla públicamente.

### f. Caso A.C (twittero opositor al gobierno de Milei)

A.C. es un joven que, al ganar Milei las elecciones en el balotaje de noviembre de 2023, abrió una cuenta en X e Instagram opositora al gobierno. En dicha cuenta, difunde diversas noticias críticas al gobierno y expresiones de personas que votaron a Milei y que en la actualidad se ven perjudicadas por las políticas de ajuste llevadas adelante por el gobierno.

A.C. compartió, como parte de su contenido habitual, el tweet de un chico que había apoyado a Milei durante las elecciones y que ahora publicaba la venta de su computadora con el objetivo de usar el dinero de la venta para arreglar cosas de la casa.

Sin embargo, este usuario, llamado Matías, le respondió diciendo que borrara el posteo y que

iba a ir a su casa a buscarlo, indagando a otros usuarios acerca de dónde vivía A.C.

Es ahí, cuando se puso en juego la maquinaria del grupo autodenominado KFC.
Los **tweets** de Matías los comienza a responder repetidamente la cuenta @juanmacilib con el nombre "Trump Shelby" quien adjunta un link al blog/página del KFC (kfcok.net), una página que tienen y donde se dedican a subir doxeos diversos. En el link compartido por @juanmacibili estaban todos los datos de A.C., los que se notaban sacados del RENAPER y un informe crediticio sobre él realizado en infoexperto. La dirección que figura allí y en su DNI es la dirección de la casa de la mamá de A.C., domicilio en el que él ya no vive.

A lo largo de todo ese día, esta cuenta respondió a numerosos tweets viejos y nuevos de la cuenta de A.C. en pos de difundir el link al blog y por ende, los datos de él.

Al día siguiente, está misma cuenta comenzó a subir posteos con fotos en este domicilio con comentarios del tipo *"¿Qué pasa que no salís? Te estamos esperando/Te estamos vigilando"*. Luego de unas horas le informan que le iba a llegar un "regalo" por pedidos ya y que lo reciba, el cual era un pedido hecho a la cadena "KFC", en un claro intento por marcar su ataque.

Durante todo ese día y el día siguiente, sonó el timbre de la casa de la familia de A.C. reiteradas veces en busca de supuestas heladeras y hornos que estaban donando.

Estas personas venían por publicaciones en grupos de Facebook que realizaba una tal "Ayelen" en las cuales se ofrecían electrodomésticos y se pedían servicios dando como dirección la de la familia de A.C. y como teléfono, el celular de él.

Cuando las personas llegaban y se comunicaban con el perfil de Facebook con el que venían hablando, la persona detrás del chat comenzaba a responder insultándolos y diciéndoles cosas como "saluda a la cámara que te estoy filmando" o afirmando que los estaba mirando por las ventanas, en un claro intento por generar enojo y violencia con quien estuviera del otro lado de la puerta.

También enviaron un camión de mudanza contratado vía Facebook el cual obviamente no había sido solicitado por A.C.

Si bien los ataques durante unos días frenaron, a la semana, Matías, el usuario que vendía su computadora y que A.C. había compartido, posteó en la red social una foto en la puerta de la casa de la mamá de A.C. y un video donde se veía a dos chicos jóvenes golpeando la puerta y tocado el timbre mientras vociferaban "que salga que salga". A las horas estas dos personas postearon una foto donde una de ellas tenía un cuchillo en la mano y otra donde se ve un arma, claramente en tono amenazante.

Este caso fue judicializado en un principio para protección del hogar de A.C. pero luego no quiso continuar con la denuncia ni seguir el proceso.

Como puede observarse estos últimos dos casos fueron ejecutados por el KFC, grupo que, parece tener como motor *doxear* y luego hostigar a quienes *twiteen* algo que los ponga en evidencia o los moleste de alguna manera. En la causa de A se vinculó a Federico Javier Gorga como titular de la "Asociación Civil de los Consumidores por la Libertad", sociedad que se utilizó para colocar el pasacalle con la firma "KFC.

Además, tienen este blog público: http://kfcok.org donde se puede visualizar *doxeos* que ocurren casi cotidianamente como respuesta a *tweets* diversos. Así aparecen *doxeados* un usuario que menciona haber cursado con Gorga, otro que hace alusión al grupo en un *space*, periodistas que los nombraron en sus canales, etc. Estos casos de *doxeo*, al menos por el momento, no encontraron luego consecuencias en la vida material por lo que no han tenido avances.

# 5. Expresión local de las violencias digitales

El seguimiento y análisis de los casos permitió identificar las particularidades que asumen las violencias digitales en el contexto local.

## Doxeo

El *doxeo* en nuestro país ocurre a través de la red social X y es llevado adelante generalmente por varones de ideología libertaria. Se suele dar como respuesta a tweets donde se cuestionan políticas del gobierno de turno liderado por Javier Milei. Han sido *doxeadas* tanto personas públicas como no públicas, pero el denominador común entre las víctimas es la expresión en redes sociales de comentarios en contra del gobierno actual.

Los usuarios que *doxean*, algunas veces en coordinación con otros y otras veces individualmente, publican datos como números de teléfono, direcciones personales o laborales, información crediticia y datos de la familia de la víctima.

La publicación de estos datos se hace incitando a otros a que los utilicen para acosar a la persona *doxeada*: comentarios como *"vayan a mandarle saludos"* cuando publican una dirección o *"escribanle para que sepa quien manda"* cuando publican un teléfono son comunes al momento del *doxeo*.

Luego, cuando efectivamente van al domicilio de la persona *doxeada* o le envían mensajes a su celular, los usuarios de X comparten la hazaña en la red social.

Al publicar números de teléfonos celulares, una práctica habitual es usar ese teléfono para solicitar servicios en facebook dando ese contacto como referencia. Así la persona *doxeada* comienza a recibir infinidad de mensajes a su celular.

## Swatting

La versión local del *swatting* en nuestro país consiste en hostigar a las personas *doxeadas* en sus domicilios con prácticas diversas.

Una modalidad común es la publicación de donaciones falsas en grupos de compraventa de Facebook. Estas personas crean un perfil falso desde el cual publican en grupos de compraventa avisos del tipo "regalo heladera a quien pueda venir hoy a retirarla". Cuando alguna persona interesada les escribe, le responden pasando la dirección de las víctimas.

Luego, quien va a buscar la donación se encuentra con que es todo mentira.

Al comunicarse con la persona de Facebook que realizó la publicación éste comienza a responder con insultos o burlas del tipo *"sonreí a la ventana que te estoy filmando... te hice venir hasta acá.. que*

*hambre que tenés para venir a buscar una heladera"*. Lo que buscan con esto es que quienes se acercan a buscar el electrodoméstico se enojen y violenten con quien vive en la casa, pensando que le hizo todo como una broma.

En estos casos la víctima no es solamente la persona *doxeada* sino que también quien va a buscar lo que se ofrece. Los victimarios, dicho expresamente en varias ocasiones, buscan humillar a las personas necesitadas.

Otra modalidad recurrente es el envío a los domicilios de servicios varios. Por ejemplo, contratan un fumigador, un flete o un camión para retirar volquetes y brindan la dirección de la víctima, solicitando abonar en el domicilio. Nuevamente, cuando las personas llegan se dan cuenta que les hicieron perder el tiempo y que no había ningún trabajo para realizar allí.

Hemos visto algunas otras expresiones donde la violencia tiene como objetivo hacer sentir amenazada a la víctima, intimidarla reforzando la idea de que al tener su dirección, tiene poder sobre ella.

En esta línea, envían comida por Pedidos Ya con el objetivo de "firmar" el ataque usando para esto la comida de la cadena rápida KFC, nombre que tiene uno de los grupos que perpetúa estos ataques.

Otras manifestación de *swatting* se dio con el envío de gusanos con tierra por Mercado Libre acompañado de la amenaza "vas a terminar así" en una clara amenaza de muerte. También, como ya mencionamos, fueron colocados pasacalles en las casas de las personas hostigadas.

## Violencia sexual

En los casos donde los ataques son contra mujeres o disidencias, aparece este tipo de violencia. Como mencionamos anteriormente, la difusión de contenido sexual o el envío de vídeos masturbándose mientras se escucha la voz de la víctima, solo sucede cuando aparece el género en el ataque.

A nivel legislación, este tipo de delitos es el que se encuentra más avanzado y donde más rápidamente suelen responder las empresas implicadas.

## SLAPP

Lo que hacen actualmente los grupos de derecha en Argentina es denunciar judicialmente a determinados usuarios de "X" por decir algo con lo que no comparten ideológicamente o que lisa y llanamente, les molesta. Así sucedió en varias oportunidades, tanto contra personas que se posicionan públicamente en "X" como también contra periodistas que comparten información en contra del gobierno de turno.

Muchas de estas acciones las lleva adelante el abogado Sarubbi Benitez, afín a Javier Milei. En los últimos meses llevaron a la justicia al periodista de Clarín Alejandro Alfie por notas que publicó y al twittero Javier Smaldone por haber compartido la nota de Crisis anteriormente mencionada, intimando a que deje de hacerlo.

## Creación de cuentas falsas en el exterior

Esta fue una nueva manera de accionar con la que nos topamos en el último tiempo. En noviembre del

11 Disponible en: https://revistacrisis.com.ar/notas/las-milicias-digitales-de-la-ultraderecha

2024, a través del robo de identidad, el grupo KFC creó una sociedad de responsabilidad limitada a nombre de tres personas a las que vienen *doxeando* y hostigando de forma virtual.

Desconocemos hasta el momento si esta es una forma habitual que tienen de operar los grupos de derecha, pero suponemos que fue hecho con el objetivo de deslegitimar la nota de revista Crisis en la cual se exponía a estos grupos[11].

La creación de esta sociedad la hicieron a través de una empresa de registro de Florida que se dedica a inscribir empresas y sociedades allá, la cual está acusada de actuar de forma fraudulenta y registrar miles de sociedades por día.

A la semana de creada, la dieron de baja nuevamente de forma fraudulenta, falsificando la firma de uno de los socios.

# 6. ¿Qué herramientas legales pueden existir en Argentina para tipificar estos delitos?

Como mencionamos anteriormente, la legislación específica sobre la violencia digital se encuentra muy poco avanzada para responder a las exigencias que los avances tecnológicos requieren. No existe tipificado en nuestro Código Penal ninguna de estas violencias concretas que mencionamos anteriormente, volviéndose obligatorio a la hora de denunciar, subsumir los hechos a los tipos penales ya existentes.

Vamos a mencionar aquí algunos que podrían servir para enmarcar estos delitos a fin de que sirva de guía para pensar la judicialización de estos casos.

## Amenazas

> *Art. 149 bis (Código Penal): "Será reprimido con prisión o reclusión de seis (6) meses a dos (2) años el que hiciere uso de amenazas para alarmar o amedrentar a una o más personas.*
> *En este caso la pena será de uno a tres años de prisión, si se emplearen armas o si las amenazas fueren anónimas.*
> *Será reprimido con prisión o reclusión de dos (2) a cuatro (4) años el que hiciere uso de amenazas con el propósito de obligar a otro a hacer, no hacer o tolerar algo contra su voluntad".*

Los casos que mencionamos en los puntos anteriores podrían enmarcarse dentro del delito de Amenazas del art. 149 bis del Código Penal. Si bien hay casos donde el *doxeo* o el *swatting* no configuran una amenaza coactiva, en la mayoría de los casos sí lo hace. Esto ocurre cuando detrás de los ataques existe una comunicación con un pedido que tiene como objetivo concreto silenciar a la persona. Por ejemplo cuando le dicen que como condición para dejar de hostigarlo tiene que abandonar las redes sociales.

## Incitación a la violencia (art. 212 Código Penal)

> *Art. 212 (Código Penal): "Será reprimido con prisión de tres a seis años el que públicamente incitare a la violencia colectiva contra grupos de personas o instituciones, por la sola incitación."*

Si bien el *doxeo* se va dando contra las personas de forma individual, si analizamos todos los casos en su conjunto, se observa que la violencia es contra un grupo de personas que conforman colectivamente

una posición política contra el gobierno actual. A su vez, como mencionamos al hablar del *swatting* y el *doxeo* a nivel local, la publicación de datos viene acompañada de una arenga a otros para hostigar a estas personas ya se yendo a la casa o enviando mensajes.

## Incitación al odio (art. 3 Ley 23.592)

> *"Serán reprimidos con prisión de un mes a tres años(...)quienes por cualquier medio alentaren o incitaren a la persecución o el odio contra una persona o grupos de personas a causa de su raza, religión, nacionalidad o ideas políticas"*

Este artículo de la Ley sobre Actos discriminatorios podría servir para encuadrar los casos de doxeo y swatting llevados adelante por los grupos de ultraderecha en las redes sociales, dado que, como mencionamos, el objetivo de estos actos es alentar e incitar la persecución contra determinadas personas en función de sus ideas políticas.

## Apología del delito (art. 213)

> *Art. 213 (Código Penal): "Será reprimido con prisión de un mes a un año, el que hiciere públicamente y por cualquier medio la apología de un delito o de un condenado por delito."*

La apología al delito podría servir para encuadrar los casos de violencia digital donde hacen mención a realizar algún tipo de ataque penalmente reprochable como también cuando se hace mención a casos que ya han sido juzgados como pueden ser los delitos de lesa humanidad ejecutados por la última dictadura cívico militar[12].

Cuando se le da curso a la judicialización de los casos a través de la apología al delito, las empresas no responden por considerar que esto es un delito de opinión y por lo tanto va contra la primera enmienda constitucional de los Estados Unidos. Así fue como en el caso de Ofelia mencionado anteriormente, hubo que aceptar una carta de condiciones de parte de Twitter para que la información remitida no sea utilizada para perseguir penalmente ni procesar al autor por el delito del art. 213 CP.

## Violación de secretos y de la privacidad (art. 153 bis y 157)

> *Art. 153 BIS (Código Penal): "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.*
>
> *La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."*
>
> *Art. 157 bis (Código Penal): "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:*
>
> *1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.*

12 https://www.mpfchubut.gov.ar/centro-de-noticias/esquel/presunta-apologia-del-delito

*2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.*

*3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. (...)"*

El delito que figura en el art. 153 bis podría ser utilizado para denunciar y encuadrar situaciones donde existieron hackeos como los que sufrió Lucila De Ponti cuando filtraron imágenes íntimas. De hecho, en ese caso, la justicia actuó bastante expeditivamente en relación al hackeo ya que Google respondió debidamente.

Actualmente, los *doxeos* perpetrados por el KFC suelen ser con los datos del RENAPER, lo que nos llevaría al artículo 157 ya que están accediendo a un registro de bancos personales. Sin embargo, como a principios del año 2024 hubo una filtración masiva de datos de RENAPER[13], eso complicaría el encuadre en el tipo penal, ya que podrían argumentar que no realizaron ningún tipo de ingreso ilegítimo.

## Ley Olimpia y Ley Belén

La Ley Olimpia (Ley 27.736) promulgada en nuestro país en octubre 2023 incorpora a la Ley de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres en los ámbitos en que desarrollen sus relaciones interpersonales (Ley 26.485) los derechos digitales.

Así es que se incorpora a los derechos protegidos de esta ley *"Que se respete su dignidad, reputación e identidad, incluso en los espacios digitales."*, esto modifica varios artículos de ley a los cuales se suma la persecución de las agresiones tanto analogicas como digitales, incorporando por ejemplo que las mismas deben cesar en el espacio digital. También define la violencia digital como *"toda conducta, acción u omisión en contra de las mujeres basada en su género que sea cometida, instigada o agravada, en parte o en su totalidad, con la asistencia, utilización y/o apropiación de las tecnologías de la información y la comunicación, con el objeto de causar daños físicos, psicológicos, económicos, sexuales o morales tanto en el ámbito privado como en el público a ellas o su grupo familiar.*

*En especial conductas que atenten contra su integridad, dignidad, identidad, reputación, libertad, y contra el acceso, permanencia y desenvolvimiento en el espacio digital o que impliquen la obtención, reproducción y difusión, sin consentimiento de material digital real o editado, intimo o de desnudez, que se le atribuya a las mujeres, o la reproducción en el espacio digital de discursos de odio misóginos y patrones estereotipados sexistas o situaciones de acoso, amenaza, extorsión, control o espionaje de la actividad virtual, accesos no autorizados a dispositivos electrónicos o cuentas en línea, robo y difusión no consentida de datos personales en la medida en que no sean conductas permitidas por la ley 25.326 y/o la que en el futuro la reemplace, o acciones que atenten contra la integridad sexual de las mujeres a través de las tecnologías de la información y la comunicación, o cualquier ciberataque que pueda surgir a futuro y que afecte los derechos protegidos en la presente ley."*

La ley Olimpia le da importancia a las empresas de redes sociales y la preservación de contenido para prueba, entendiendo que son parte fundamental de este entramado. Así el artículo 12 dice:

*"Incorpórase como apartado a.9. del artículo 26 de la ley 26.485, el siguiente texto:*

13 https://chequeado.com/el-explicador/filtracion-de-datos-personales-en-el-renaper-que-es-y-que-conse cuencias-puede-tener/

*a.9. Ordenar por auto fundado, a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, de manera escrita o electrónica la supresión de contenidos que constituyan un ejercicio de la violencia digital o telemática definida en la presente ley, debiendo identificarse en la orden la URL específica del contenido cuya remoción se ordena. A los fines de notificación de la medida del presente inciso se podrá aplicar el artículo 122 de la ley 19.550.*

*La autoridad interviniente en el caso deberá solicitar a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, el aseguramiento de los datos informáticos relativos al tráfico, a los abonados y contenido del material suprimido, que obren en su poder o estén bajo su control, para las acciones de fondo que correspondan, durante un plazo de noventa (90) días que podrá renovarse una única vez por idéntico plazo a pedido de la parte interesada. Se deberá ordenar mantener en secreto la ejecución de dicho procedimiento mientras dure la orden de aseguramiento.*

*La autoridad podrá, a requerimiento de parte y únicamente para la investigación de las acciones de fondo que correspondan, solicitar a las requeridas que revelen los datos informáticos de abonados que obren en su poder o estén bajo su control e igualmente los relativos al tráfico y al contenido del material suprimido mediante auto fundado de acuerdo a los mecanismos de cooperación interna y/o procedimientos previstos en el marco de las normas y tratados sobre cooperación internacional vigentes."*

La Ley Belén es un proyecto de ley que busca modificar el Código Penal a fin de que aparezca tipificado como delito la difusión de contenido sexual de mujeres sin su consentimiento. Resulta destacable de este proyecto el que refiere a la incorporación del artículo 155 bis el cual quedaría redactado de la siguiente forma:

*"Se aplicará prisión de ocho meses a un año y el doble de la multa establecida en el artículo 155° a quien, por cualquier medio, sin autorización de la víctima o mediando engaño, videograbe, audiograbe, fotografíe, filme o elabore, documentos con contenidos de desnudez, naturaleza sexual o representaciones sexuales. Se aplicará prisión de tres meses a tres años y el doble de la multa establecida en el art. 155 a quien, por cualquier medio, y sin autorización de la víctima difunda, publique, envíe o de cualquier manera ponga al alcance de terceros documentos con contenidos de desnudez o naturaleza sexual o representaciones sexuales que el autor haya recibido de la persona afectada, o que el autor haya producido u obtenido de la persona afectada con o sin mediar su consentimiento.*

*Se aplicará prisión de ocho meses a un año y el doble de la multa establecida en el art. 155 a quien, habiendo recibido del autor del párrafo anterior o de terceras personas o teniendo en su poder por cualquier circunstancia distinta a la descrita en el primer párrafo, los documentos allí referidos, por cualquier medio, y sin consentimiento de la víctima los difunda, publique, envíe o de cualquier manera ponga al alcance de terceros.*

*Se aplicará prisión de ocho meses a un año y el doble de la multa establecida en el art. 155° a quien, por cualquier medio, y sin autorización de la víctima, difunda, publique, envíe o de cualquier manera ponga al alcance de terceros, documentos con contenidos de desnudez, naturaleza sexual o representaciones sexuales que se hayan elaborado con el uso de las tecnologías de la información y la comunicación, o de la inteligencia artificial, y no correspondan con la persona que es retratada, señalada y/o identificada en los mismos."*

En los casos de violencia digital donde la violencia sexual está presente y hay filtración de contenido sexual la aplicación de la Ley Olimpia podría resultar un elemento clave para perseguir a los atacantes.

Sin embargo, lo cierto es que por más que la ley en cuestión obligue a las autoridades a solicitar acciones a las empresas de redes sociales, estas en muchas oportunidades omiten tales solicitudes.

En cuanto a la Ley Belén, todavía es un proyecto y no se encuentra sancionada, por lo tanto no podría aplicarse en ningún caso.

## Difusión no autorizada de imágenes o grabaciones intimas (art. 74 Código Contravencional de CABA)

En la Ciudad de Buenos Aires se encuentra tipificado tanto la difusión no autorizada de imágenes o grabaciones íntimas como así también el hostigamiento digital, ambos a través del Código Contravencional de la CABA.

> *ART. 74 (Código Contravencional de CABA): "Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de transmisión de datos, páginas web y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con una multa de cuatrocientas (400) a mil novecientas cincuenta (1950) unidades fijas o cinco (5) a quince (15) días de trabajo de utilidad pública o con tres (3) a diez (10) días de arresto. El consentimiento de la víctima para la difusión, siendo menor de 18 años, no será considerado válido.*
>
> *Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta.*
>
> *Acción dependiente de instancia privada con excepción de los casos donde la víctima sea menor de 18 años de edad.*
>
> *No configura contravención el ejercicio del derecho a la libertad de expresión."*

## Hostigamiento digital (art. 75 Código Contravencional de CABA)

> *Art. 75 (Código Contravencional de CABA): "Hostigamiento digital - Quien intimide u hostigue a otro mediante el uso de cualquier medio digital, siempre que el hecho no constituya delito, es sancionado con multa de ciento sesenta (160) a ochocientas (800) unidades fijas, tres (3) a diez (10) días de trabajo de utilidad pública, o uno (1) a cinco (5) días de arresto."*

Esta contravención se encuentra agravada al doble cuando el hostigamiento es anónimo y cuando es ejecutado en arreglo con dos o más personas.

## Convenio de Budapest

El Convenio de Budapest es el primer instrumento internacional que trata de manera específica aspectos relacionados con el ciberdelito. Fue sancionado en noviembre de 2001 por el Consejo de Europa y entró en vigencia en 2004. Desde 2017 Argentina lo aprobó como parte de su legislación.

Este convenio es un marco normativo, es decir, actúa como referencia al establecer principios y compromisos para los países firmantes respecto de la persecución del cibercrimen y la cooperación internacional. No estipula sanciones para los países que no lo implementen en su totalidad.

Si bien este Convenio es importante, no es suficiente. Sin leyes nacionales y poderes ejecutivos que acompañen, no hay coerción suficiente para que se cumplan las obligaciones ni se garantice cabalmente los derechos que busca resguardar. El Convenio de Budapest es claro en impulsar a los firmantes a que

tomen "medidas legislativas" en línea con las disposiciones del convenio pero lo cierto es que siempre se termina dependiendo de leyes locales.

En la práctica, una empresa puede negarse a brindar información, atenerse a que la ley de su país de orígen no se lo impone o alegar sus propias políticas de privacidad y confidencialidad, dificultando el proceso de recolección de evidencia.
El primer protocolo de este Convenio busca penalizar la propaganda racista y xenófoba a través de los sistemas informáticos como así también las amenazas.

El segundo protocolo, intenta dar respuesta al desafío de obtener evidencia electrónica, problema importante que surge cuando se judicializan estos casos porque mucha información se encuentra almacenada en servidores extranjeros.

Aunque el Convenio obliga a los Estados Parte a sancionar leyes que persigan los delitos informáticos y se brinde cooperación internacional para el marco probatorio, lo cierto es que depende de la legislación que efectivamente se lleve luego adelante en cada país para poder avanzar en este sentido.

## 8. Problemas, desafíos y propuestas

A través del trabajo de las causas antes mencionadas en este Informe notamos que existen algunos problemas bastante concretos a la hora de llevar a cabo la investigación de delitos que se gestan en la esfera virtual.

Desde ya que hay jurisdicciones que han avanzado en capacitaciones y formación sobre esta materia y también hay equipos técnicos que cuentan con personal y con insumos que son de mucha utilidad.

Un primer problema que existe a la hora de solicitar medidas de prueba en este tipo de casos es la falta de contestación de las plataformas digitales. Como fue mencionado en el apartado de "*Análisis de Casos*", la empresa de X (ex Twitter), perteneciente al empresario Elon Musk desde el año 2022, dejó de responder los pedidos de la justicia para localizar a quienes son investigados por cometer delitos. Lo que nos lleva a observar en la actualidad un paradigma en el cual las empresas de redes sociales se encuentran por encima de los estados y sus soberanías.

En la actualidad existen herramientas normativas que buscan obligar a las plataformas digitales a que respondan los pedidos judiciales. Un ejemplo claro es el Convenio de Budapest (artículo 18.1.b.) el cual habilita a las autoridades competentes para ordenar que "un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios".

También está la Ley Federal de Comunicaciones almacenadas (Federal Stored Communications Act) del Código de los Estados Unidos (Título 18, Sección 2703 c) que es el fundamento que tenemos para solicitarle a las empresas con asiento en el país norteamericano la información requerida. Sin embargo, no es una obligación legal. Por lo que si la empresa conforme sus políticas (localización o actividad de la cuenta, tipo de caso investigado en nuestro país, etc.) decide no compartir la información con las autoridades argentinas, se debe enviar una solicitud de asistencia jurídica para que un juez de Estados Unidos emita una orden en esa dirección.

En este sentido, creemos que es de vital importancia que nuestro país efectivice el Convenio de Budapest ratificado y sancione más normas en esta materia. En esa línea creemos que una vía para paliar los

problemas referidos a la falta de cooperación de los proveedores de servicios digitales podría ser la sanción de una norma (o varias) que regule un marco normativo para aquellas. Esta norma debería tener criterios de responsabilidad mínima donde se defina en qué casos las proveedoras deberán cooperar, en qué plazos y por qué canales, incluyendo a proveedores de servicios VPN, y todo esto, más allá de dónde estén radicadas sus oficinas. Se podría pensar también en la obligación de constituir un domicilio en Argentina para poder operar acá como sucede en Brasil.
De esta manera, con una normativa local que fortalezca la responsabilidad de las empresas en cuestión, se podrán tener mayores herramientas tanto para solicitar medidas como también para imponer sanciones en el caso en que no se cumpla con los requerimientos judiciales. Caso contrario, no tendremos ni siquiera un marco para exigir el comportamiento que necesitamos por parte de estas compañías y la impunidad para cometer delitos a través de las redes irá en aumento.

En Francia recientemente fueron imputados varios ejecutivos de la empresa de mensajería Telegram debido a su negativa a colaborar en una investigación sobre actividades ilícitas organizadas a través de su plataforma.[14]

También en Brasil hace pocos meses la justicia del país ordenó a X que brindara información sobre unas cuentas que estaban siendo investigadas por expresiones antidemocráticas y difusión de *fake news* dentro de la causa *"milicias digitales"*. Como la empresa se negó a hacerlo, se le impuso una multa diario a lo que Musk respondió sacando a su representante legal del país, lo cual no está permitido en Brasil ya que allí todas las plataformas de redes sociales deben contar con al menos un representante legal con quien se pueda contactar.

Frente a esto, el juez Moraes Alexandre de Moraes, del Supremo Tribunal Federal de Brasil(STF), ordenó la suspensión de X en el país, debiendo las empresas de internet bloquear el acceso a la plataforma desde las IP brasileras. Finalmente, gracias a la intervención del presidente de Brasil, Lula Da Silva, Musk terminó pagando la multa y colocando un representante legal en el país[15].

Estos casos ilustran el problema con las plataformas digitales las cuales, independientemente de la gravedad del delito investigado, se niegan a compartir información crucial para las investigaciones. La falta de cooperación por parte de estas empresas no solo obstaculiza la justicia, sino que también subraya la necesidad de marcos legales sólidos y actualizados.

Otro problema que es usual en este tema es el resguardo de la prueba. La información que se suele necesitar para probar los delitos cometidos se encuentra en la propia plataforma y muchas veces los proveedores de los servicios pueden eliminarla ya sea por acción del propio usuario (borrado de fotos, publicaciones, mensajes, eliminación de cuenta), por acción de las empresas, por razones económicas o de otra naturaleza o por el propio paso del tiempo.

Es por eso que es crucial que tanto el Poder Judicial interviniente como los abogados litigantes tengamos herramientas para solicitar la preservación de la información de interés[16], más allá de que los proveedores estén dispuestos u obligados a responder requerimientos de autoridades judiciales radicadas en el extranjero.

El Título 18, Sección 2703 (f) del Código de los Estados Unidos estipula que las empresas con asiento

14 https://www.bbc.com/mundo/articles/c89wq2y4k01o

15 https://www.lapoliticaonline.com/internacionales/musk-acata-la-decision-de-la-justicia-brasilena-y-deb era-eliminar-la-cuenta-de-cerimedo/

16 https://www.mpf.gob.ar/ufeci/files/2021/07/UFECI-2020-Gui%CC%81a-de-Evidencia-Digital.pdf

en ese país podrán preservar información por un plazo de 90 días, renovables una vez (Hay empresas que igual la preservan más tiempos, Google un año o Microsoft 180 días). Además la Convención de Budapest en el artículo 16 establece que "las Partes adoptarán las medidas legislativas o de otro tipo (...) para: 1) ordenar o imponer de otro modo la conservación inmediata de datos electrónico especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdidas o de modificación." De esta manera, se puede solicitar la preservación de la información, que no implica pedirla ni tampoco obliga a la empresa a hacerlo, pero sí asegura que esté disponible cuando sea pedida vía oficio judicial o exhorto. Al igual que el punto anterior, esta obligación también debería estar regulada normativamente a nivel local para así tener mayores herramientas con las cuales solicitar el resguardo informático.

Sin embargo, y más allá de todo lo desarrollado en este punto, queda pendiente además de un mayor desarrollo en el área, que la sociedad en general, y la política en particular, comience a ver con seriedad la violencia con causa ideológica que prolifera y se coordina a través de las redes sociales y que luego se traduce en la vida cotidiana de ciudadanos. Caso contrario, vamos a permitir que los límites se sigan corriendo y que, incluso quienes son víctimas, naturalicen el silenciamiento y las amenazas por querer expresar opiniones diversas: lo que constituye un cercenamiento de la libertad de expresión y por ende de la construcción política en el país.

*Investigaciones abiertas para la construcción de evidencia* es fruto de un trabajo colaborativo desarrollado durante el 2025 desde el espacio de intercambio *ataques en entorno digitales* donde diversas organizaciones buscamos retroalimentar los procesos de investigación y litigio, sistematizar experiencias y metodologías que contribuyan al aprendizaje colectivo, y potenciar donde sea posible estrategias conjuntas de incidencia.

En los distintos artículos se indaga en los aportes de la investigación ciudadana al terreno judicial, ya sea mediante reconstrucciones con datos extraídos de fuentes abiertas o coberturas colaborativas durante manifestaciones. Se resaltan la potencia y los desafíos técnicos, institucionales y político-metodológicos de estas prácticas de intervención publica a través de la información recolectada y analizada de forma colectiva e interdisciplinaria.

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay