LA ILICITUD EN LA PRUEBA TECNOLÓGICA

*Lucía Solange Torres Sánchez**

SUMARIO: Resumen. Introducción. 1. La prueba ilícita en el sistema penal chileno. 2. Las tecnologías como generadoras de pruebas. 3. Consideraciones finales. Bibliografía.

RESUMEN

El presente trabajo visualiza la necesidad de integrar las nuevas tecnologías en las evidencias presentadas en el proceso penal sin menoscabar la protección a los derechos fundamentales. El aporte de este trabajo radica en ofrecer un marco analítico que articula la necesidad de adaptar los principios tradicionales de la prueba a las innovaciones tecnológicas que permiten el análisis forense de datos, la geolocalización, la vigilancia mediante dispositivos digitales y la aplicación de inteligencia artificial, asegurando que la búsqueda de la verdad en la investigación penal no se realice mediante medios probatorios ilegítimos, a costa de derechos fundamentales y de la protección de la vida privada.

Palabras claves: Prueba ilícita, tecnología, derechos fundamentales.

INTRODUCCIÓN

El reconocido jurista chileno Agustín Squella Narducci sostiene que *el derecho es un fenómeno que no pertenece a la naturaleza, sino a la sociedad, o sea, que se trata de algo que el hombre hace o produce con un cierto fin; que es algo, además, que contiene normas o que tiene que ver preferentemente con normas; que, por lo mismo, la experiencia que todos tenemos del derecho es, ante todo, una experiencia normativa; y que, en fin, cuando se estudia derecho, lo que se estudia, de preferencia,*

*Licenciada en Ciencias Jurídicas y Sociales, Universidad de Chile. Magíster en Derecho Público, Universidad Santo Tomás.

El presente trabajo constituye una elaboración derivada del Trabajo Final Aplicado, presentado como requisito para la obtención del grado de Magíster en Derecho Público en la Universidad Santo Tomás.

es un conjunto de normas vigentes en un lugar y tiempo dados, por medio de las cuales los hombres regulan sus comportamientos, establecen derechos y obligaciones recíprocos, prevén posibles conflictos y dan a estos, cuando se producen, un curso de solución que no pasa simplemente por la aplicación de la ley del más fuerte, y consienten, en fin, en que tales normas puedan ser auxiliadas, a efectos de su cumplimiento, por el uso de la fuerza socialmente organizada[1]. Esta perspectiva destaca la función del derecho como regulador de la conducta social y la posibilidad de imponer su cumplimiento mediante la coacción. Se infiere de dicha definición que el derecho en sí debe evolucionar para responder a los desafíos que se plantean en el tiempo, siendo en estos tiempos la globalización y la transformación digital un gran reto para el Derecho. Sin embargo, esta evolución en nuestra sociedad no puede significar una disminución en la protección de los derechos fundamentales, sino que debe ser una adaptación que nos permita incorporar los avances tecnológicos sin poner en riesgo la defensa de estos derechos[2], en otras palabras, encontrar un equilibrio que nos permita avanzar con la tecnología, pero sin olvidar lo que realmente importa: proteger y garantizar los derechos básicos de todas las personas.

La llegada del internet, con ello la globalización y de todas las tecnologías de la información ha cambiado por completo la forma en que creamos, compartimos y utilizamos los datos. En este nuevo escenario, proteger nuestra privacidad se ha vuelto algo mucho más complicado porque nuestra información personal ahora es como un tesoro que muchas empresas quieren aprovechar para fines comerciales, y que los gobiernos pueden utilizar para vigilarnos. Es como si, de repente, nuestra vida privada estuviera expuesta en un mundo donde los datos valen más que nunca, y tenemos que ser conscientes de cómo cuidarlos.

En el ámbito de derecho procesal el desarrollo de nuevas tecnologías ha transformado la obtención, valoración y exclusión de la prueba en el proceso, desafiando los principios clásicos de legalidad, debido proceso y derechos fundamentales, generando intensos debates en torno a la licitud de pruebas obtenidas con tecnologías intrusivas o sin consentimiento[3].

---

[1]Squella Narducci. A. (2000). *Introducción al Derecho. Derecho, Sociedad y Normas de Conducta*. Editorial Jurídica de Chile. 29 y 30.

[2]Murillo De La Cueva, P. L. (2004). *Derechos fundamentales y avances tecnológicos: Los riesgos del progreso*, Boletín mexicano de Derecho Comparado, México, v. 37, n° 109, 71-110. Consultado el 4 de febrero de 2025. [http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332004000100003&lng=es&nrm=iso].

[3]Coloma Correa, L; Agüero San Juan, C. y Lira Rodríguez, R. (2021). *Tecnología para decidir hechos en procesos judiciales*. Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile. Vol. 10 Núm. 1, 111-143.

En el sistema penal chileno, el artículo 276 del Código Procesal Penal consagra el principio de exclusión de pruebas obtenidas con vulneración de derechos fundamentales. En este contexto, en el presente trabajo se analizan diversas doctrinas, tales como la del fruto del árbol envenenado, el principio de proporcionalidad, la teoría de la fuente independiente, la buena fe y el descubrimiento inevitable, las que buscan equilibrar la eficacia en la obtención de pruebas y el respeto a las garantías procesales.

Además, se subraya la importancia de la educación jurídica en materia digital, que permita comprender y aplicar las normativas en un entorno cada vez más complejo. En definitiva, el estudio plantea que la evolución normativa y práctica debe acompañar el avance tecnológico, garantizando una justicia que sea eficiente y respetuosa de los derechos fundamentales. Asimismo, aborda la problemática de la admisibilidad de la prueba tecnológica ilícita y el debate constante generado en la tensión entre la eficiencia en la investigación penal en búsqueda de la verdad y la protección de los derechos fundamentales.

1. LA PRUEBA ILÍCITA EN EL SISTEMA PENAL CHILENO

Por prueba ilícita debe entenderse por aquella prueba obtenida o practicada con vulneración de derechos fundamentales[4]. En el sistema penal chileno, el principio de exclusión de la prueba ilícita se encuentra consagrado en el artículo 276 del Código Procesal Penal, el que sanciona la ineficacia de la prueba ilícita en sede de admisibilidad.

El manejo de la prueba ilícita en Chile busca el equilibrio entre procesos judiciales justos y la protección de manera efectiva de los derechos fundamentales, por tanto, se puede concluir que "solo la verdad obtenida con el respeto a esas reglas básicas constituidas por los derechos fundamentales puede estimarse como jurídicamente válida. Lo que se trata de conocer en un proceso judicial no es lo verdadero en sí, sino lo justo y, por tanto, la verdad solo tiene valor en la medida en que forma parte de lo justo. Si esto es así y todo indica que lo es, los derechos fundamentales marcan el camino que debemos seguir para alcanzar un conocimiento que sea válido en el ámbito judicial"[5].

Por lo que, si una prueba se obtiene de manera ilegítima, no debería ser admitida. Sin perjuicio a lo anterior, los tribunales han ido introduciendo ciertos matices y excepciones que permiten, en algunos casos, evaluar si

---

[4]Miranda Estrampes, M. (2010)." La Prueba Ilícita: La Regla de Exclusión Probatoria y sus Excepciones". España. *Revista Catalana de Seguretat Pública*. 133.

[5]Vives Anton, T. (2004) "Doctrina constitucional y reforma del proceso penal", Jornadas sobre la justicia penal, citado por Jacobo López Barja de Quiroga en *Tratado de Derecho procesal penal*. España. Thompson Reuter Aranzadi, 947.

esa prueba pudiese ser válida bajo condiciones específicas[6]. Este debate está en constante evolución, buscando siempre la eficacia, pero sin olvidar que el respeto a los derechos humanos debe estar en el centro de todo. Entre los criterios desarrollados por la jurisprudencia para determinar la exclusión de la prueba ilícita, se destacan:

1. Doctrina del fruto del árbol envenenado: Si una prueba es fruto de un acto ilegal, todo lo que derive de ella pierde validez, incluso si se obtuvo siguiendo los procedimientos correctos, en tanto constituyan una consecuencia de la ilegalidad original[7].
2. Principio de proporcionalidad: Se pondera en cada caso concreto varios factores, se ha admitido la posibilidad de evaluar la ilicitud en casos donde la transgresión es menor frente a un interés preponderante, como la persecución de delitos graves, impidiendo el sacrificio del interés en la averiguación de la verdad cuando los elementos probatorios hayan sido obtenidos con sacrificio de bienes de menor entidad[8].
3. Teoría de la fuente independiente: Establece que, si la misma prueba pudo haberse obtenido por medios lícitos y de manera independiente a la vulneración original, podría ser admitida en el proceso[9].
4. Teoría de la buena fe: Permite la utilización de pruebas obtenidas de manera ilícita cuando se demuestra que la infracción fue cometida sin intención dolosa por parte del órgano investigador. En el sistema penal chileno siendo la protección de garantías fundamentales la finalidad directa de la regla de exclusión, impide relativizar su aplicación y vigencia atendiendo la simple creencia de un funcionario, de estar actuando conforme a derecho al obtener la prueba[10], sin perjuicio de lo anterior, es posible advertir jurisprudencia en sentido contrario, Rol 5816-2019, Nulidad, Corte Suprema, en que se sostiene que la

---

[6]Sentencia de la Corte Suprema, Rol 20160-2019. Ministerio Público Antofagasta con José Miguel González Rosales, de 7 de octubre del 2019. Nulidad. Excepción del vínculo atenuado.

Sentencia de la Corte Suprema Rol 33252-2019. Ministerio Público con Juan Cristóbal André Guarda Alveal, de 21 de febrero del 2020. Nulidad. Proporcionalidad, tolerancia mientras no se vulnere el núcleo esencial del derecho.

Sentencia de la Corte Suprema Rol 5816-2019. Ministerio Público con Sandoval Morales, de 16 de abril de 2019. Nulidad. Teoría de la buena fe.

[7]Lopez Barja De Quiroga, J. (2001). *Instituciones del derecho procesal penal*. Argentina. Ediciones Jurídicas Cuyo, 284.

[8]Horvitz, M.I. y López, J. (2004), *Derecho procesal penal chileno*, Tomo II. Santiago, Editorial Jurídica de Chile, primera edición, 175.

[9]Correa Robles, C. (2023). *Efectos Reflejos De La Regla De Exclusión De Prueba Ilícita: Una Conclusión (No Tan) Obvia. Revista Ius Et Praxis*, año 29, N°1, 86-108.

[10]Correa Robles, C. (2018). *La buena fe del agente como excepción a la aplicación de la regla de exclusión – Derecho Estadounidense y Derecho Chileno* . Latin American Legal Studies. Volumen 2 (2018). Consultado el 13 de febrero de 2025 [https://lals.uai.cl/index.php/rld]

buena fe constituye un elemento que debe ser sopesado para descartar la ilicitud del obrar de los agentes estatales.

5. Descubrimiento inevitable: Si se puede demostrar que la evidencia habría sido descubierta inevitablemente por medios lícitos, cuya obtención conforme a derecho resultare esperable, atendida la existencia de un curso causal hipotético lícito, más no realizado.

En el contexto del proceso penal chileno, conforme a la jurisprudencia analizada[11], las doctrinas que permiten matizar la regla de exclusión no operan todas con la misma fuerza ni pueden aplicarse de manera automática. La del fruto del árbol envenenado tiene un rol central, pues busca proteger derechos fundamentales que son esenciales en un juicio justo, de igual forma las otras teorías, como la proporcionalidad, la buena fe o el descubrimiento inevitable, todas deben aplicarse con mucha cautela y solo después de un análisis detallado de las circunstancias del caso. Por

---

[11]Sentencia Corte Suprema, Rol N°49714-2016, 15 de septiembre de 2016. Considerando 4°, doctrina: "No encuadra en la teoría del fruto del árbol envenenado la prueba de un delito que se comete de manera flagrante con motivo u ocasión de una actuación ilegal previa de los policías para obtener prueba de otro delito".

Sentencia Corte Suprema, Rol N° 1741-2010, 25 de mayo de 2010. Considerando 23°. Doctrina "No hay nexo causal si el conocimiento de los hechos se había obtenido con anterioridad mediante una fuente dependiente, y la evidencia ilícitamente obtenida sirvió para confirmar sospechas previas y focalizar la investigación en determinadas imputadas". Teoría Fuente Independiente.

Considerando 22°. Doctrina: "Para resolver una solicitud de exclusión de prueba, debe tenerse en cuenta, entre otros aspectos, que la jurisprudencia alemana ha dado acogida a la excepción a la teoría de los frutos del árbol envenenado, fundada en la ponderación de los intereses en conflicto, que se ampara en el principio de proporcionalidad". Teoría de la proporcionalidad.

Sentencia Corte Suprema, Rol 49714-2016, 15 de septiembre de 2016. Considerando 4°. Doctrina "No encuadra en la teoría del fruto del árbol envenenado, la prueba obtenida de un delito que se comete de manera flagrante con motivo u ocasión de una actuación ilegal previa de policías para obtener prueba de otro delito".

Sentencia Corte Suprema, Rol N° 5816-2019, 16 de abril de 2019. Considerando 6°. Doctrina "La infracción en la obtención de la declaración del imputado, en la que señala que en su vivienda mantenía más droga, carece de sustancialidad desde que el fiscal ya había instruido a los policías registrar el inmueble, a lo que accedió el acusado". Teoría Descubrimiento Inevitable.

Sentencia Corte Suprema, Rol N°42335-2017, 28 de diciembre de 2017. Considerando 9°a 12°. Doctrina "La doctrina del vínculo atenuado resulta pertinente si se reitera la confesión una vez ya efectuada la lectura de derechos por los agentes policiales, porque ello desvanece o difumina el vínculo con la supuesta ilegalidad previa". Teoría del vínculo atenuado.

Sentencia Corte Suprema, Rol N°23300-2018, 4 de diciembre de 2018. Considerando 3° al 7°. Doctrina "Los policías actúan de buena fe al creer que la autorización judicial de entrada y registro a un departamento comprende la bodega anexa a este, donde se mantiene la droga que se comercializa a terceros". Teoría de la Buena Fe.

Rodríguez Vega, M. (2022). *La prueba ilícita en la jurisprudencia de la Corte Suprema*. Editorial Rubicón. Chile.

ello, tanto las partes como los jueces deben actuar con especial responsabilidad: quienes presentan las pruebas deben respaldar sus argumentos con hechos concretos, y quienes las evalúan deben realizar un examen riguroso que evite justificar prácticas ilegales. El objetivo final no debe perderse de vista: asegurar que el respeto por los derechos fundamentales no quede solo en el papel, sino que se exprese de forma real y efectiva en cada decisión judicial.

2. LAS TECNOLOGÍAS COMO GENERADORAS DE PRUEBAS

En la búsqueda de la verdad para establecer una decisión judicial existe un proceso de investigación donde se insertan diferentes diligencias, las que, según las circunstancias del caso concreto, pueden implicar una afectación a derechos fundamentales. Las innovaciones tecnológicas[12] han generado nuevas formas de obtención de prueba, algunas de estas colisionan con derechos como el de la intimidad y el secreto de las comunicaciones, y con el principio de autodeterminación informativa[13-14]. Así, se hace imprescindible un análisis que permita comprender tanto los beneficios como los riesgos que estas tecnologías representan en el ámbito procesal.

Entre las nuevas metodologías de obtención de prueba, encontramos las siguientes:

INFORMÁTICA FORENSE

Se utilizan herramientas especializadas para la extracción y análisis de datos de dispositivos electrónicos (computadoras, smartphones, tabletas) y redes. Esto incluye la recuperación de información borrada y la reconstrucción de actividades digitales, lo que es crucial en investigaciones de ciertos delitos, siendo imprescindible la necesidad de aplicar protocolos especiales de actuación de los órganos encargados de su levantamiento,

---

[12]Azuaje, M. y Contreras, P. (2021). *Inteligencia artificial y Derecho: Desafíos y perspectivas*. 1° edición. Chile. Editorial Tirant lo Blanch.

[13]La autodeterminación informativa se ha entendido como el control que ofrece a las personas respecto del uso por terceros de información acerca de ellas mismas.

[Contreras, Pablo. (2020). *El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena*. Estudios constitucionales, 18(2), 87-120. Disponible en https://dx.doi.org/10.4067/S0718-52002020000020008]

En el contexto chileno, la Ley 19.628 sobre Protección de la Vida Privada regula la protección de datos personales, estableciendo derechos y obligaciones para garantizar la privacidad y el control de la información personal.

[14]Pérez-Ugena, M. (2024). *El derecho al olvido frente a buscadores en internet. El derecho a la autodeterminación informativa como fundamento del derecho al olvido*. Editorial Dykinson, España. 57-75.

traslado, custodia y análisis, así, velar por la integridad e inalterabilidad de la información contenida en soportes informáticos[15].

El allanamiento de dispositivos electrónicos sin una orden judicial ha sido calificado por varios tribunales en el mundo como una clara violación al debido proceso que provoca inseguridad jurídica al afectarse eventualmente el derecho a la privacidad e intimidad y al alterar la cadena de custodia que acarreará la nulidad de esa prueba en juicio por ilícita. Aun así, existen casos en los que se ha aceptado la evidencia obtenida por particulares, sin que intervenga directamente el Estado[16], estableciendo una distinción muy importante en lo que respecta a la exclusión de pruebas.

En Chile, conforme con lo indicado en el apartado anterior, se ha optado por un enfoque de exclusión con matices[17], sin perjuicio de ello, se debe cumplir estrictamente los protocolos, pues el valor legal y técnico de la evidencia digital depende en gran medida del proceso de recopilación y preservación que se haya seguido.

GEOLOCALIZACIÓN Y VIGILANCIA[18]

El uso de dispositivos como GPS ("Global Positioning System", que en español se traduce como "Sistema de Posicionamiento Global"), cámaras ocultas y software espía ha revolucionado la capacidad de las autoridades para rastrear y recolectar información relevante en investigaciones penales. Sin embargo, cuando estos datos se recolectan sin el consentimiento de las personas, surge una inquietud muy seria: ¿estamos vulnerando el derecho

---

[15]Santelices,V. (2014). *Tratamiento de la evidencia contenida en soportes informáticos como prueba en el proceso penal*. Revista Actualidad Jurídica N° 29, Universidad del Desarrollo-Chile. Pág.539-552.

[16]Sentencia Cámara de Apelaciones –Décimo Circuito– de fecha 17 de agosto del año 2018, 900 F.3d 636 "United States of America, Plaintiff-Appellee v. Henry Franklin REDDICK, Defendant-Appellant". Consultado el 10 de febrero de 2025 en [https://www.eldial.com/nuevo/nuevo_diseno/v2/fallo4.asp?id=52269&base=14&referencia=604&Total_registros2_1=5847&buscar=%7Bbuscar%7D&resaltar=%7Bbuscar%7D]

[17]La problemática de la prueba ilícita se encuentra vinculada e incide en el robustecimiento del Estado de Derecho, de la tutela efectiva, de la igualdad ante la ley y de los derechos fundamentales de las personas (…) Tal es ese desarrollo y peso que tiene la prueba ilícita en el proceso penal, que cualquiera con cercanía a la rutina de nuestros juzgados de garantía y tribunales de juicio oral en lo penal, fácilmente se percatará que las discusiones acerca de la licitud de las actuaciones de investigación y persecución, junto con las referentes a la valoración de los antecedentes y de la prueba –según la etapa del proceso–, superan con holgura a la aplicación del derecho penal sustantivo, que ha sido relegado a controversias aisladas y ocasionales.

Rodríguez Vega, M. (2022). *La Prueba Ilícita en la Jurisprudencia de la Corte Suprema*. Primera edición, Chile, Rubicón Editores. 12-18.

[18]Palomino Ángeles, E. y Villalpando, A. (2023). *Revista Alegatos*, núm. 114, México, mayo-agosto de 2023. Departamento de Derecho de la Universidad Autónoma Metropolitana Unidad Azcapotzalco. 101-122.

a la vida privada? Si bien en la jurisprudencia nacional no se proscribe por completo el uso de herramientas de seguimiento (GPS, drones, cámaras), se exige un escrutinio estricto de su legalidad y proporcionalidad. Cuando la vigilancia carece de sustento normativo claro o invade esferas íntimas sin justificación, los tribunales han estado dispuestos a considerarla una vulneración del artículo 19 N°4 de la Carta Fundamental. Por el contrario, cuando la medida se apega a la ley, persigue un fin necesario (como la seguridad pública o el control laboral legítimo) y se implementa acotadamente, tiende a ser avalada judicialmente. Cada caso concreto ha aportado matices, pero en conjunto delinean una tendencia: la vigilancia sin consentimiento es la excepción, no la regla, y solo se tolera bajo estrictas garantías y supervisión judicial o legal. Así, además, debe indagar si la medida persigue un fin legítimo indispensable, y si afecta la privacidad en la medida mínima necesaria para lograr dicho fin.

Principio de legalidad: Los jueces exigen que la recolección de datos personales tenga sustento en la ley o en el consentimiento del afectado. Por ejemplo, en el caso de los drones de vigilancia de la Municipalidad de Las Condes[19] (año 2017), los recurrentes alegaban que la captura de imágenes por drones carecía de autorización de los titulares y violaba la Ley 19.628. Sin embargo, tanto la Corte de Apelaciones de Santiago como la Corte Suprema estimaron que existía una base legal suficiente: las facultades de seguridad comunal que la Ley Orgánica de Municipalidades confiere a los alcaldes (art. 4° letra j) y art. 5° letra i) de la Ley 18.695)[20]. Con ese fundamento, la Corte Suprema confirmó que la instalación de drones por la municipalidad no era ilegal, pues se enmarcaba en sus competencias legales y respetaba las normas técnicas aplicables[21] (por ejemplo, operando con inspectores acreditados por la Dirección de Aeronáutica Civil). De modo similar, en otros casos se ha valorado el consentimiento expreso: en un caso de teletrabajo, donde un empleador implementó un sistema de control horario vía aplicación móvil con geolocalización y foto, los tribunales estimaron que al haberse pactado dicha modalidad en el contrato o anexo, no había actuar ilegal ni arbitrario[22].

---

[19]Sentencia Corte Apelaciones de Santiago, Rol N° 34360-2017, 21 de agosto de 2017.

[20]Malamud, S. (2018). "Videovigilancia y privacidad. Consideraciones en torno a los casos 'Globos' y 'Drones'". *Revista Chilena de Derecho y Tecnología*, Vol. 7 Núm. 2, 137-162. Consultado el 14 de febrero de 2025. https://dx.doi.org/10.5354/0719-2584.2018.49097

[21]El artículo 20 de la Ley N° 19.628, sobre protección de datos personales, establece que los organismos públicos pueden tratar datos personales sin necesidad de consentimiento del titular, si se cumplen ciertas condiciones. Por tanto, si se delegase la operación del sistema a una entidad privada, se desdibujaría el carácter público de la función y, con ello, se perdería la legitimidad que justifica la excepción al consentimiento.

[22]Sentencia Corte de Apelaciones de Santiago, Rol 6459-202, 16 de noviembre de 2021.

En síntesis, si la recopilación de datos de ubicación carece de respaldo normativo o consentimiento, los tribunales tienden a considerarla contraria al artículo 19 N°4 de la Constitución.

Principio de necesidad y finalidad legítima: Aun contando con base legal, la medida debe responder a una finalidad legítima concreta y ser necesaria para alcanzarla. Los tribunales han reconocido finalidades como la seguridad pública, la prevención del delito o el cumplimiento de obligaciones contractuales como razones que pueden justificar ciertas intrusiones en la privacidad. En el caso de los drones de Las Condes, el fin invocado fue la seguridad ciudadana en espacios públicos ante problemas de delincuencia; la Corte Suprema señaló que no se acreditó ninguna afectación concreta a derechos en el contexto de vigilancia en lugares públicos, por lo que la acción de protección no podía prosperar. De igual manera, en el caso de los globos de vigilancia adquiridos por las municipalidades de Las Condes y Lo Barnechea[23] (año 2016), la finalidad de prevención del delito se consideró legítima, pero la Corte Suprema puso énfasis en delimitar claramente el ámbito de la vigilancia para proteger la intimidad de los vecinos. En su fallo unánime, el máximo tribunal revocó la prohibición absoluta que había impuesto la Corte de Apelaciones (la que había ordenado bajar los globos) argumentando que "no resulta aceptable prohibir de manera absoluta la captación de toda clase de imágenes […] pues no resulta aceptable postular algún tipo de derecho sobre el espacio aéreo"[24]. En lugar de suprimir la medida, la Corte Suprema optó por autorizarla con restricciones orientadas por la necesidad: solo se podría grabar lo indispensable para la seguridad, evitando intromisiones injustificadas. Así, ordenó que las cámaras "se limiten a la captación en espacios públicos, y en espacios privados solo cuando se trate del seguimiento de un hecho que pueda constituir un ilícito"[25].

Esto último muestra que la vigilancia sobre lugares de privacidad resguardada no se justifica salvo en casos extremos, por ejemplo, persecución en flagrancia de un delincuente. En contextos laborales, igualmente se evalúa la necesidad de la medida: la Corte Suprema ha reconocido que el empleador tiene una "facultad legítima de controlar y vigilar el cumplimiento

---

[23]Sentencias de Corte de Apelaciones de Santiago. Roles N°81627-2015 y N°82289-2015, ambas del 4 de marzo de 2016.

Sentencia Corte Suprema. Roles N°18458-2016 y N°18481-2016, ambas del 1 de junio de 2016.

Sentencias Corte de Apelaciones de Santiago. Rol N°34360-2017, 21 de agosto de 2017.

Sentencia Corte Suprema. Rol N°38527-2017, 11 de diciembre de 2017.

[24]Sentencia Corte Suprema, Rol N° 18481-2016, 01 de junio de 2016.

[25]Microjuris Chile al Día (3 de junio 2016*). Corte Suprema revocó sentencia que ordenó retirar los globos de televigilancia en Las Condes y Lo Barnechea. ¿Qué dice el fallo?* Consultado el 21 de marzo de 2025. https://aldiachile.microjuris.com/2016/06/03/corte-suprema-revoco-sentencia-que-ordeno-retirar-los-globos-de-televigilancia-en-las-condes-y-lo-barnechea-que-dice-el-fallo/

de las obligaciones laborales"[26] de sus trabajadores, lo que puede incluir mecanismos de geolocalización, siempre que sean necesarios para ese fin (por ejemplo, monitorear vehículos o registrar asistencia). En un caso de Minera Escondida[27] (año 2017), la empresa sancionó a conductores por ralentizar maquinaria basándose en datos de GPS; los trabajadores impugnaron la medida por vulnerar su privacidad, pero la Corte Suprema descartó la vulneración, razonando que el uso del GPS estaba ligado a un fin lícito (supervisar el trabajo) y que no se probó ninguna afectación distinta a la necesaria para ese control.

Principio de proporcionalidad: Incluso cuando hay un fin legítimo, la interferencia en la vida privada se debe realizar del modo menos invasivo posible. Los fallos frecuentemente subrayan este equilibrio. En el caso de Minera Escondida, la Corte Suprema explicitó que la supervisión mediante GPS es admisible solo si se emplea de forma proporcional y con la mínima intrusión en la libertad y privacidad de los trabajadores, acotada al ámbito y horario laboral, "con exclusión de... tiempo y espacios privados destinados al descanso"[28]. Es decir, el sistema de seguimiento no podía extenderse a vigilar al trabajador fuera de sus funciones. Además, la sentencia destacó como factores a favor de la proporcionalidad el carácter fiable del dispositivo (margen de error mínimo) y el hecho de haber sido consentido por los propios afectados dentro de la relación laboral. De igual forma, en la sentencia de los globos de vigilancia, la Corte Suprema impuso límites temporales y materiales muy claros para minimizar la intrusión: exigió destruir las grabaciones tras 30 días, salvo que registren un delito y garantizar el acceso de cualquier ciudadano a las imágenes captadas de sí mismo[29].

Estas condiciones de destruccción periódica de datos y posibilidad de control social sobre ellos, reflejan una aplicación del principio de proporcionalidad, evitando acumulación innecesaria de datos y reduciendo el riesgo de usos abusivos. En el caso de los drones, la proporcionalidad se logró, en opinión de los tribunales, mediante la delimitación previa del espacio de operación solo a ciertos sectores públicos y la observancia de un Manual de Procedimientos que impedía intromisiones arbitrarias. La Corte de Apelaciones y la Suprema coincidieron en que "la conducta reprochada no resulta ilegal ni arbitraria, sin que se haya demostrado una afectación… de las garantías constitucionales… en los espacios públicos

---

[26]Diario Constitucional (13 de septiembre de 2017). *CS rechaza protección de trabajadores sancionados por empresa minera utilizando GPS como prueba*. Consultado el 21 de marzo de 2025. https://www.diarioconstitucional.cl/2017/09/13/cs-rechaza-proteccion-de-trabajadores-sancionados-por-empresa-minera-utilizando-gps-como-prueba/

[27]Sentencia Corte Suprema, Rol N° 15403-2017, 4 de septiembre de 2017.

[28]Sentencia Corte Suprema, Rol N° 15403-2017. 4 de septiembre de 2017, considerando 10°.

[29]Sentencia Corte Suprema Rol N° 18481-2016, Corte Suprema, numeral 3, parte resolutiva.

donde se ha implementado el plan"[30]. En otras palabras, mientras el uso de drones se restringiera a vigilar plazas, calles y lugares abiertos al público, donde la expectativa de privacidad es menor y no existiera evidencia de abusos, como grabaciones de la vida íntima, la medida se consideraba proporcionada al objetivo de seguridad.

PRUEBAS OBTENIDAS MEDIANTE INTELIGENCIA ARTIFICIAL (IA)[31]

La inteligencia artificial, por medio de algoritmos de reconocimiento facial y del análisis de patrones de comportamiento, puede identificar situaciones delictivas con una precisión sorprendente. No obstante, el uso de estas herramientas sin una regulación clara ha generado controversia[32,33], ya que muchos temen que pueda afectar el derecho de cada individuo a controlar su propia información personal. Entre los derechos fundamentales que se ven más afectados por el uso de la inteligencia artificial, podemos destacar aquellos que tocan aspectos esenciales de nuestra vida y dignidad como seres humanos, como es el valor de la privacidad (derechos a la vida privada, a la honra, a la protección de los datos personales, a la inviolabilidad del hogar y de las comunicaciones privadas).

Las soluciones pueden ir desde: *generar nuevas e importantes facultades que se interpreten como parte del objeto de algunos derechos fundamentales ya reconocidos y, en su caso, se plasmen en las leyes que los desarrollen*[34], o bien, acudir a la técnica de los derechos implícitos que la jurisprudencia ya ha reconocido en nuestros tribunales[35], además, de reconocer normativamente neuroderechos, actualmente existe un

---

[30]Colegio de Abogados (14 de diciembre de 2017). *Suprema confirmó rechazo de recurso de protección y Las Condes podrá seguir con drones de vigilancia*. Consultado el 20 de marzo de 2025. https://colegioabogados.cl/suprema-confirmo-rechazo-recurso-proteccion-las-condes-podra-seguir-drones-vigilancia/

[31]Yáñez García-Bernalt, I. (2024). "La inteligencia artificial en el proceso penal: eficiencia versus garantías". *Ius Et Scientia*, España, Vol. 10, Nº 2, 80-100. Consultado el 10 de febrero de 2025. https://doi.org/10.12795/IESTSCIENTIA.2024.i02.04

[32]Asociación por los Derechos Civiles (2017*). La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos*. Consultado el 23 de marzo de 2025. http://bit.ly/2tksUil.

[33]Garrido Iglesias, R. y Becker Castellaro, S. (2017). "La biometría en Chile y sus riesgos". *Revista Chilena de Derecho y Tecnología*, Vol. 6, n° 1, 67-91. Consultado el 21 de marzo de 2025. https://dx.doi.org/10.5354/0719-2584.2017.45825

[34]Presno Linera, M.A. (2023): *Derechos fundamentales e inteligencia artificial*. España. Editorial Marcial Pons, 84, citado por Peña Torres, M. y Sagredo, MJ. (2024). *Inteligencia artificial y derechos fundamentales*.

[35]Peña Torres, M. y Sagredo, MJ. (2024)." Inteligencia artificial y derechos fundamentales: impacto en los derechos de la privacidad". *Revista de Derecho Actualidad Jurídica de la Universidad del Desarrollo*, n° 50. Ediciones Universidad del Desarrollo. 80.

proyecto de ley en Chile[36], el que se tramita desde el 2020, que regula el uso de neurotecnologías y protege los siguientes derechos: los derechos a la privacidad mental; a la identidad y autonomía personal; al libre albedrío y a la autodeterminación; al acceso equitativo a la aumentación cognitiva y a la producción de sesgos de algoritmos o procesos automatizados de toma de decisiones[37]. Es importante destacar que Chile es el primer país en abordar los neuroderechos a nivel constitucional en la reforma del año 2021[38].

El documental de Netfix "El Gran Hackeo" relata el escándalo de Cambridge Analytica, dejando de manifiesto que todo lo que hacemos en el mundo digital va dejando un rastro, y que nuestras vidas están sometidas a una vigilancia y control, en donde empresas de alta tecnología pueden constituir una enorme amenaza para nuestros derechos humanos, al ser estos datos objeto de análisis de comportamientos y manipulación por medio de ingeniería social. La divulgación no autorizada de datos de Facebook por Cambridge Analytica ha vulnerado el derecho a la privacidad de los usuarios revelando que en la era digital los datos se han convertido en el activo más valioso que grupos de poder explotan con fines inescrupulosos[39]. Organizaciones de derechos humanos como "Amnistía

---

[36]Número de boletín 13828-19. Proyecto de ley sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías.

[37]El neurobiólogo Rafael Yuste ha comparado esta iniciativa con tomar medidas proactivas antes de que la tecnología "lea y manipule" la mente humana de forma masiva, evitando así repetir errores cometidos con avances previos (como sucedió con la falta de regulación inicial de las redes sociales o de la genética) [Montes, R. (8 de octubre de 2020). *Chile, laboratorio mundial de los neuroderechos*. Diario El País. España. Consultado el 19 de marzo de 2025. https://elpais.com/ciencia/2020-10-08/chile-laboratorio-mundial-de-los-neuroderechos.html]

El investigador Pedro Maldonado, de la Universidad de Chile, observa que los proyectos en discusión "no explican bien qué es la actividad mental o la conexión neuronal", y considera esa precisión fundamental para delimitar el alcance de la ley. [Guzmán, L. (31 de marzo de 2022). *Chile, pionero en la protección de los "neuroderechos".* El Correo de la UNESCO. Consultado el 19 de marzo de 2025. https://courier.unesco.org/es/articles/chile-pionero-en-la-proteccion-de-los-neuroderechos]

En una columna publicada por juristas del Centro de Filosofía del Derecho de la Universidad de Valparaíso señala "debilidades jurídicas" en la iniciativa y sostiene que "se está legislando sin entender bien lo que se quiere proteger" [Zúñiga Fajuri, A. Villavicencio Miranda, L. y Salas Venegas, R. (11 de diciembre de 2020). *¿Neuroderechos? Razones para no legislar*. CIPER Chile. Consultado el 19 de marzo de 2025. https://www.ciperchile.cl/2020/12/11/neuroderechos-razones-para-no-legislar/]

[38]Ley N°21.383. Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas. "*El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella".*

[39]Sánchez Ballesteros, C. (2020). *Nada es privado: un documental sobre Cambridge Analytica*. Consultado el 22 de marzo de 2025. https://www.academia.edu/45050838/Nada_es_privado_un_documental_sobre_Cambridge_Analytica

Internacional" advierten que la vigilancia corporativa masiva, donde empresas tecnológicas acumulan cantidades inéditas de datos acerca de las personas, amenaza la esencia misma del derecho a la privacidad, lo que evidencia la necesidad de reforzar las leyes de protección de datos. En Europa, por ejemplo, se invoca el Reglamento General de Protección de Datos como modelo para responsabilizar a las empresas y prevenir la minería de datos sin control[40].

Se expone en dicho documental cómo las grandes corporaciones tecnológicas han adoptado un modelo de negocio basado en la vigilancia constante de nuestras actividades en línea, un fenómeno que la académica Shoshana Zuboff denomina "capitalismo de vigilancia". Según Zuboff, la película logra mostrar lo que significa vivir bajo las condiciones del capitalismo de vigilancia, donde cada acción se reutiliza como materia prima para datos de comportamiento. Estos datos se extraen de forma invisible, de modo que los usuarios ni siquiera son conscientes de cuándo ocurre ni pueden oponer resistencia[41]. En suma, El Gran Hackeo ha sido analizado como un llamado de atención acerca de la urgente necesidad de proteger la privacidad en la era del *Big Data* y de actualizar el marco legal para salvaguardar los datos personales de los usuarios. Además, alerta respecto del potencial uso indebido del análisis de datos por parte de los gobiernos, lo que podría comprometer derechos fundamentales y la integridad de los procesos democráticos.

En el ámbito del proceso investigativo penal, el abogado Roberto Navarro-Dolmestch sostiene que: *el ciberrastreo puede ser usado en términos preventivos (por ejemplo, PredPol) anticipando la probabilidad de ocurrencia de hechos delictivos (en el modelo alemán, con la Schleppnetzfahndung), sobre todo en materia de terrorismo o tráfico de drogas (el llamado Smart law enforcement); como una técnica de investigación de delitos ya cometidos o en el proceso de adopción de decisiones judiciales*[42].

Si en la acusación presenta como prueba el resultado de un algoritmo o *software* de IA, por ejemplo, un informe de reconocimiento facial o un puntaje de riesgo delictual, la defensa tiene derecho a examinar críticamente cómo se obtuvo ese resultado. La lógica o diseño del algoritmo debe ser comprensible para las partes, de modo de garantizar el derecho de defensa y contradicción respecto de dicha prueba. Si el funcionamiento

---

[40]Natt, S. (25 de julio 2019). *Why 'The Great Hack' is just the tip of the iceberg. Amnesty International UK*. Consultado el 24 de marzo de 2025. https://www.amnesty.org.uk/blogs/campaigns/the-great-hack

[41]Cadwalladr, C. (20 de julio 2019). *The Great Hack: the film* that goes behind the scenes of the Facebook data scandal. The Guardian. Consultado el 24 de marzo de 2025. https://www.theguardian.com/uk-news/2019/jul/20/the-great-hack-cambridge-analytica-scandal-facebook-netflix

[42]Navarro Dolmestch, R. (2024). "Ciberrastreo Analítico: *Web Scraping* y *Big Data* como Técnicas de Investigación en el Derecho Procesal Penal Chileno". *Revista de Derecho Actualidad Jurídica de la Universidad del Desarrollo*, n° 50. Ediciones Universidad del Desarrollo. 306.

del sistema de IA es opaco, la defensa podría verse impedida de impugnar sus conclusiones, generándose una situación de indefensión. De allí que autores subrayan la necesidad de una adecuada auditoría y transparencia de los algoritmos empleados en el proceso penal[43]. En última instancia, si persisten dudas razonables acerca de la confiabilidad o imparcialidad de una prueba algorítmica, deberá primar el *in dubio pro reo*, es decir, debe optarse por la presunción de inocencia[44]. Existe un riesgo inherente al uso de inteligencia artificial en la justicia que es el sesgo algorítmico. Los sistemas aprenden de datos históricos que pueden contener prejuicios, reproduciéndolos en sus resultados. Por tanto, cualquier uso de algoritmos en la fase probatoria debe ser sometido a escrutinio: es indispensable verificar que los datos de entrenamiento sean de calidad y representativos, y que el modelo no incorpore discriminaciones prohibidas, pues de lo contrario se comprometen derechos fundamentales de igualdad y no discriminación. La eventual opacidad algorítmica choca con la exigencia de transparencia propia del debido proceso. De hecho, se ha advertido que los sistemas opacos merman la transparencia del proceso penal, al haber una "pérdida de control" sobre la técnica de procesamiento de la información. Si no es posible seguir paso a paso cómo la IA analizó los datos, queda en duda la exactitud y confiabilidad del resultado obtenido[45].

En línea con lo anterior, la doctrina sugiere incorporar principios como la transparencia algorítmica, la no discriminación y la trazabilidad en cualquier sistema automatizado empleado por policías o tribunales. Asimismo, se enfatiza que la IA debe concebirse como herramienta de apoyo, nunca como sustituto del juzgador humano en la valoración de la prueba[46-47].

---

[43]Pérez Estrada, M. J. (2021). La inteligencia artificial como prueba científica en el proceso penal español. Revista Brasileira de Direito Processual Penal, vol. 7, núm. 2. Consultado el 21 de marzo de 2025. https://www.redalyc.org/journal/6739/673972089017/html/

[44]Suárez, J. (2011). "Inferencia razonable, probabilidad de verdad y conocimiento más allá de toda duda razonable". *Principia Iuris*. Vol. 16, págs. 307-330. Consultado el 21 de marzo de 2025. https://bit.ly/3x7eLFn

[45]Vivar Vera, Juliana (2021). "La sentencia penal, el juez y el algoritmo: ¿Las nuevas tecnologías serán nuestros próximos jueces?". *Revista chilena de derecho y tecnología*, vol. 10, n.1, págs. 231-269. Consultado el 20 de marzo de 2025. https://dx.doi.org/10.5354/0719-2584.2021.58785

[46]Pérez Estrada, M. J. (2021). "La inteligencia artificial como prueba científica en el proceso penal español". *Revista Brasileira de Direito Processual Penal*, vol. 7, n.2. Consultado el 23 de marzo de 2025. https://www.redalyc.org/journal/6739/673972089017/html/

[47]Vivar Vera, Juliana (2021). "La sentencia penal, el juez y el algoritmo: ¿Las nuevas tecnologías serán nuestros próximos jueces?". *Revista chilena de derecho y tecnología*, vol.10, n.1, págs. 231-269. Consultado el 20 de marzo de 2025. https://dx.doi.org/10.5354/0719-2584.2021.58785

La monitorización y análisis de interacciones en redes sociales, aplicaciones de mensajería y otras plataformas digitales permiten reconstruir cronologías y relaciones que pueden ser determinantes en el esclarecimiento de hechos. La literatura especializada denomina esta práctica inteligencia en redes sociales o SOCMINT (del inglés Social Media Intelligence), entendida como el uso de técnicas de recolección y análisis de perfiles, fotografías, videos, conversaciones, contactos, comentarios y todo tipo de contenido generado en plataformas digitales[48] que permiten trazar mapas de conexiones entre individuos a partir de sus interacciones en línea[49].

Las redes sociales públicas aportan evidencia en juicios penales, así es como en el 2017 la Corte Suprema de Chile validó varias fotografías publicadas en Facebook como prueba contra acusados de robo, rechazando la alegación de que eran obtenidas ilícitamente. El tribunal razonó que cualquier contenido publicado en Facebook bajo la configuración "público" no puede considerarse privado, por lo que no está protegido por la garantía constitucional de inviolabilidad de las comunicaciones[50]. Esta decisión confirmó que las publicaciones visibles para cualquiera en redes sociales se pueden utilizar legítimamente como evidencia, por cuanto quien las divulga renuncia a reclamar privacidad acerca de ellas. En la práctica, estas pruebas han servido para comparar fotos de sospechosos en redes con imágenes de cámaras de seguridad en investigaciones, fortaleciendo la identificación de imputados.

Las aplicaciones de mensajería también generan evidencias relevantes. Un dictamen de la Contraloría General de la República (sede administrativa) sostuvo que un investigador "se encuentra facultado para valorar los audios o capturas de pantalla de conversaciones, mensajes o imágenes de redes sociales... como uno de los elementos que pueden servir de base a sus conclusiones"[51] Ello refleja una tendencia a aceptar que las conversaciones digitales privadas, obtenidas y presentadas correctamente, puedan ser consideradas medios de prueba en casos graves, por ejemplo, acoso sexual o laboral investigado administrativamente, siempre y cuando se entreguen de manera voluntaria por alguno de los participantes de la conversación. En mismo sentido se pronuncia la Corte de Apelaciones

---

[48]Díaz P. y Gemetto J. (2023). *Ciberpatrullaje: los límites borrosos de la vigilancia policial en Uruguay.* Datysoc. Consultado el 20 de marzo de 2021 https://datysoc.org/informe-ciberpatrullaje/

[49]Gómez Agudelo, D. Acevedo Valencia, J. y Aguirre Espinosa, J. (2021). *Autenticidad y debido proceso en los mensajes de Whatsapp: Una revisión en los casos de divorcio. Revista chilena de derecho y tecnología*, Vol. 10, n°2, págs 123-148. Consultado el 20 de marzo de 2025. https://dx.doi.org/10.5354/0719-2584.2021.58039

[50]Sentencia Corte Suprema, rol N° 3-2017, 27 de febrero de 2017.

[51]Dictamen Contraloría General de la República, E288163N22, 15 de diciembre de 2022.

de Santiago[52], en causa de Protección confirmada posteriormente por la Corte Suprema.

El artículo 19 Nº 5 de la Constitución Política asegura "la inviolabilidad... de toda forma de comunicación privada", disponiendo que las comunicaciones y documentos privados solo pueden ser interceptados, abiertos o registrados en los casos y formas que la ley establezca. La evidencia digital en el proceso penal, ya sea la interceptación de llamados telefónicos, mensajes o correos electrónicos requiere una autorización judicial previa, o bien, que esta evidencia sea presentada por uno de los interlocutores de la conversación. La jurisprudencia ha enfatizado que la verdad judicial se debe alcanzar sin sacrificar garantías básicas; la llamada doctrina del fruto del árbol envenenado, de modo que, si la policía obtuviera cierta evidencia digital ilegalmente, contaminaría también las pruebas derivadas de ella. Por ejemplo, si se accede sin autorización a un correo y a partir de allí se descubren otros datos, todo ese conjunto probatorio podría ser anulado.

Una correcta utilización de evidencia digital en el proceso penal exige equilibrar la eficacia investigativa con el respeto a los derechos fundamentales del imputado. Chile, a nivel normativo, proporciona un marco flexible que admite estos nuevos medios de prueba, pero a la vez impone condiciones: obtenerlos legítimamente, preservarlos íntegros y permitir a la defensa confrontarlos adecuadamente.

Un ejemplo emblemático es el denominado Caso Hermosilla o Caso Audios (aún en desarrollo al momento de escribir este trabajo), el que se trata de una presunta red de tráfico de influencias, sobornos y delitos tributarios, revelada en parte gracias a un registro de audio filtrado y a la incautación de cientos de miles de mensajes de texto del principal imputado, todas estas evidencias digitales permitieron destapar una presunta red de corrupción, pero su manejo ha debido sortear objeciones de privacidad y secreto profesional, así como desafíos logísticos debido a la enorme cantidad de datos involucrados. Este caso demuestra que las comunicaciones digitales pueden ser el núcleo de una investigación penal exitosa, siempre que las autoridades actúen dentro del marco legal (allanamientos autorizados, peritajes técnicos, etc.) y que los tribunales ejerzan control acerca de la pertinencia y licitud de lo presentado.

3. CONSIDERACIONES FINALES

El uso de tecnologías como medios de prueba en el ámbito penal representa un avance significativo en términos de precisión y eficiencia investigativa. No obstante, su incorporación plantea desafíos relevantes en la protección

[52]Sentencia Corte de Apelaciones de Santiago, Rol N°4504-2021, 18 de enero de 2022.

de los derechos fundamentales. Toda vez que las evidencias tecnológicas pueden ser obtenidas en contextos difusos (no siempre tiene un origen, modo y momento de obtención claramente identificables), lo que dificulta la identificación de eventuales vulneraciones de garantías. Asimismo, se presentan problemas de transparencia, especialmente cuando no se conoce con claridad cómo fue procesada la información. A ello se suman riesgos asociados a la ruptura de la cadena de custodia, la posible falta de autenticidad del contenido y la existencia de sesgos algorítmicos, que podrían derivar en imputaciones erróneas o decisiones injustas.

Además, la aplicación de las teorías de exclusión se vuelve más compleja en el entorno digital, ya que se dificulta la identificación de ilicitud del origen (por ejemplo, el caso de redes abiertas) o que por su naturaleza intangible se torne complicado demostrar si un dato fue "fruto" directo de una infracción o si su obtención fue autónoma y en el caso de existencia de una única diligencia ilegal podría conllevar la contaminación masiva de miles de datos.

Se puede afirmar que la utilización de tecnologías debe ir acompañada de un análisis riguroso que prevenga posibles excesos o vulneraciones a los derechos fundamentales, como el derecho a la privacidad, derecho a la intimidad y el debido proceso, siendo fundamental que nuestro marco normativo evolucione para adaptarse de manera efectiva a estas nuevas herramientas, contemplando salvaguardias específicas que aseguren que la obtención y el uso de la evidencia digital se realicen respetando los principios de legalidad, proporcionalidad y seguridad jurídica.

Asimismo, resulta esencial establecer protocolos de la cadena de custodia y la pericia técnica, con el fin de garantizar la integridad, autenticidad y trazabilidad de la evidencia digital, lo que es esencial para evitar cuestionamientos a su validez y, por esta razón, para evitar que su admisión vulnere derechos fundamentales.

Se infiere la importancia de la educación jurídica en materia de tecnología. Los abogados deben incluir en su formación el estudio de las nuevas tecnologías y sus implicaciones. Tal formación debe estar orientada hacia la comprensión integral del fenómeno digital y la valoración crítica de sus consecuencias en el sistema jurídico tradicional[53].

En definitiva, se debe lograr un balance que permita aprovechar las ventajas de las tecnologías en la investigación judicial sin comprometer los derechos individuales. Para ello, es necesario actualizar continuamente las metodologías forenses, reforzar el marco legal vigente y promover una formación constante en protección de datos y derechos fundamentales.

---

[53]Cicero. N.K. (2018). "Innovar la enseñanza del derecho. ¿Solo se trata de tecnologías de la información y comunicación?". *Revista Pedagogía Universitaria y Didáctica del Derecho*. Vol. 5. Núm. 2 (2018), 91-109.

BIBLIOGRAFÍA

Asociación por los Derechos Civiles. (2017). *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos*. Disponible en http://bit.ly/2tksUil

Azuaje, M. y Contreras, P. (2021). *Inteligencia artificial y Derecho: Desafíos y perspectivas*. 1° edición. Chile. Editorial Tirant Lo Blanch.

Cadwalladr, C. (20 de julio 2019). *The Great Hack: the film that goes behind the scenes of the Facebook data scandal*. The Guardian. Disponible en https://www.theguardian.com/uk-news/2019/jul/20/the-great-hack-cambridge-analytica-scandal-facebook-netflix

Cicero. N.K. (2018). *Innovar la enseñanza del derecho. ¿Solo se trata de tecnologías de la información y comunicación?*. Revista Pedagogía Universitaria y Didáctica del Derecho. Vol. 5. Núm. 2 (2018).

Colegio de Abogados. (14 de diciembre 2017). *Suprema confirmó rechazo de recurso de protección y Las Condes podrá seguir con drones de vigilancia*. Disponible en https://colegioabogados.cl/suprema-confirmo-rechazo-recurso-proteccion-las-condes-podra-seguir-drones-vigilancia/

Coloma Correa, L; Agüero San Juan, C. y Lira Rodríguez, R. (2021). *Tecnología para decidir hechos en procesos judiciales*. Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile. Vol. 10 Núm. 1.

Comisión Biblioteca del Congreso Nacional. *La Sociedad, el Derecho y el Pensamiento Político. Guía de Formación Cívica,* Chile, 4° edición. Disponible en [https://www.bcn.cl/formacioncivica/detalle_guia?h=10221.3/45670#:~:text=El%20Derecho%20es%20un%20sistema,relevancia%20jur%C3%ADdica%2C%20pudiendo%20imponerse%20coactivamente.]

Correa Robles, C. (2018). *La buena fe del agente como excepción a la aplicación de la regla de exclusión – Derecho Estadounidense y Derecho Chileno* . Latin American Legal Studies, volumen 2. Disponible en [https://lals.uai.cl/index.php/rld]

Correa Robles, C. (2023). *Efectos Reflejos de la Regla de Exclusión de Prueba Ilícita: Una Conclusión (No Tan) Obvia*. Revista Ius et Praxis, Talca, Chile. Disponible en [http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071800122023000100086&lng=es&nrm=iso]

Contreras, P. (2020). *El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena*. Estudios constitucionales, Vol.18, n°2. Disponible en https://dx.doi.org/10.4067/S0718-52000202000020008

Diario Constitucional. (13 de septiembre 2017). *CS rechaza protección de trabajadores sancionados por empresa minera utilizando GPS como prueba*. Disponible en https://www.diarioconstitucional.cl/2017/09/13/cs-rechaza-proteccion-de-trabajadores-sancionados-por-empresa-minera-utilizando-gps-como-prueba/

Díaz P. y Gemetto J. (2023). *Ciberpatrullaje: los límites borrosos de la vigilancia policial en Uruguay*. Datysoc. Disponible en: https://datysoc.org/informe-ciberpatrullaje/

Garrido Iglesias, R. y Becker Castellaro, S. (2017). *La biometría en Chile y sus riesgos. Revista chilena de derecho y tecnología* Disponible en https://dx.doi.org/10.5354/0719-2584.2017.45825

Gómez Agudelo, D. Acevedo Valencia, J. y Aguirre Espinosa, J. (2021). *Autenticidad y debido proceso en los mensajes de Whatsapp: Una revisión en los casos de divorcio. Revista chilena de derecho y tecnología*. Disponible en https://dx.doi.org/10.5354/0719-2584.2021.58039

Guzmán, L. (31 de marzo de 2022). *Chile, pionero en la protección de los "neuroderechos"*. El Correo de la UNESCO. Disponible en https://courier.unesco.org/es/articles/chile-pionero-en-la-proteccion-de-los-neuroderechos

Horvitz, M.I. y López, J. (2004), *Derecho procesal penal chileno*, Tomo II, primera edición. Santiago, Editorial Jurídica de Chile.

Leturia. F. (2016). *Sentencias Destacadas 2016. Comentario De Sentencia: Uso De Globos De Vigilancia*. Chile, Universidad Diego Portales.

Lopez Barja De Quiroga, J. (2001). *Instituciones del derecho procesal penal*. Argentina. Ediciones Jurídicas Cuyo.

Malamud, S. (2018). *Videovigilancia y privacidad. Consideraciones en torno a los casos "Globos" y "Drones"*. Revista chilena de derecho y tecnología, Chile. Vol 7, n°2.

Microjuris Chile al Día. (3 de junio 2016). *Corte Suprema revocó sentencia que ordenó retirar los globos de televigilancia en Las Condes y Lo Barnechea. ¿Qué dice el fallo?* Disponible en https://aldiachile.microjuris.com/2016/06/03/corte-suprema-revoco-sentencia-que-ordeno-retirar-los-globos-de-televigilancia-en-las-condes-y-lo-barnechea-que-dice-el-fallo/

Miranda Estrampes, M. (2010). *La Prueba Ilícita: La Regla de Exclusión Probatoria y sus Excepciones*. España. Revista Catalana de Seguretat Pública.

Montes, R. (8 de octubre de 2020). *Chile, laboratorio mundial de los neuroderechos*. Diario El País. España. Disponible en https://elpais.com/ciencia/2020-10-08/chile-laboratorio-mundial-de-los-neuroderechos.html

Murillo De La Cueva, P. L. (2004). *Derechos fundamentales y avances tecnológicos: Los riesgos del progreso*, Boletín mexicano de Derecho Comparado, México, volumen 37, n° 109. Disponible en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041863320040001000003&lng=es&nrm=iso

Natt, S. (25 de julio 2019). *Why 'The Great Hack' is just the tip of the iceberg.* Amnesty International UK. Disponible en https://www.amnesty.org.uk/blogs/campaigns/the-great-hack

Navarro Dolmestch, R. (2024*). Ciberrastreo Analítico: Web Scraping y Big Data como Técnicas de Investigación en el Derecho Procesal Penal Chileno*. Revista de Derecho Actualidad Jurídica de la Universidad del Desarrollo, n° 50. Ediciones Universidad del Desarrollo.

Palomino Ángeles, E. y Villalpando, A. (2023). *Revista Alegatos*, núm. 114, México, mayo-agosto de 2023. Departamento de Derecho de la Universidad Autónoma Metropolitana Unidad Azcapotzalco.

Peña Torres, M. y Sagredo, MJ. (2024). *Inteligencia artificial y derechos fundamentales: impacto en los derechos de la privacidad*. Revista de Derecho Actualidad Jurídica de la Universidad del Desarrollo, n°50. Ediciones Universidad del Desarrollo.

Pérez Estrada, M. J. (2021). *La inteligencia artificial como prueba científica en el proceso penal español*. Revista Brasileira de Direito Processual Penal, vol. 7, n.2. Disponible en https://www.redalyc.org/journal/6739/673972089017/html/

Pérez-Ugena, M. (2024). *El derecho al olvido frente a buscadores en internet. El derecho a la autodeterminación informativa como fundamento del derecho al olvido*. España, Editorial Dykinson.

Rodríguez Vega, M. (2022). *La prueba ilícita en la jurisprudencia de la Corte Suprema*. 1° edición, Chile. Editorial Rubicón.

Sánchez Ballesteros, C. (2020). *Nada es privado: un documental sobre Cambridge Analytica*. Disponible en https://www.academia.edu/45050838/Nada_es_privado_un_documental_sobre_Cambridge_Analytica

Santelices,V. (2014). *Tratamiento de la evidencia contenida en soportes informáticos como prueba en el proceso penal*. Revista Actualidad Jurídica N° 29, Universidad del Desarrollo-Chile.

Squella Narducci. A. (2000). *Introducción al Derecho. Derecho, Sociedad y Normas de Conducta*. Chile. Editorial Jurídica de Chile.

Suárez, J. (2011). "*Inferencia razonable, probabilidad de verdad y conocimiento más allá de toda duda razonable*". Principia Iuris. (16). Disponible en https://bit.ly/3x7eLFn

Valle Muñoz, F. (2023). *Las Redes Sociales como medio de prueba en el proceso laboral*. Revista de Estudios Jurídico Laborales y de Seguridad Social (REJLSS), España, Edit. Servicio de Publicaciones y Divulgación Científica de la Universidad de Málaga. Disponible en [https://revistas.uma.es/index.php/REJLSS/article/view/16217/16780]

Vivar Vera, Juliana. (2021). La sentencia penal, el juez y el algoritmo: ¿Las nuevas tecnologías serán nuestros próximos jueces?. Revista chilena de derecho y tecnología, vol. 10, n.1, págs. 231-269. Disponible en https://dx.doi.org/10.5354/0719-2584.2021.58785

Vives Anton, T. (2004). *Doctrina constitucional y reforma del proceso penal*, Jornadas sobre la justicia penal, citado por Jacobo López Barja de Quiroga en *Tratado de Derecho procesal penal*. España. Editorial Thompson Reuter Aranzadi.

Yáñez García-Bernalt, I. (2024). *La inteligencia artificial en el proceso penal: eficiencia versus garantías*. Ius Et Scientia, España, Volumen 10, nº 2. Disponible en [https://doi.org/10.12795/IESTSCIENTIA.2024.i02.04]

Zúñiga Fajuri, A., Villavicencio Miranda, L., & Salas Venegas, R. (11 de diciembre de 2020). *¿Neuroderechos? Razones para no legislar*. CIPER Chile. Disponible en https://www.ciperchile.cl/2020/12/11/neuroderechos-razones-para-no-legislar/]