

LA TRANSPARENCIA ALGORÍTMICA COMO DIMENSIÓN DEL DERECHO DE ACCESO A LA INFORMACIÓN

CARMEN MILAGROS VELARDE KOECHLIN*
Universidad de Salamanca, España

LUIS FELIPE VELARDE KOECHLIN** †
Universidad de Lima, Perú

Recibido: 19 de marzo del 2026 / Aceptado: 4 de mayo del 2026

doi: <https://doi.org/10.26439/iusetpraxis2026.n061.8701>

RESUMEN. Este artículo analiza la transparencia algorítmica como una dimensión digital del derecho de acceso a la información en el Perú. Ante la automatización estatal y el uso de sistemas como Curia y ElecclA, surge el riesgo del efecto de caja negra y de sesgos que derivan en discriminación algorítmica. Con base en la Constitución política y el referente interamericano *Claude Reyes vs. Chile*, en esta investigación se sostiene que la explicabilidad es esencial para fiscalizar el poder tecnológico del Estado. El estudio aborda la mitigación de sesgos como un objetivo de justicia social armonizándolo con los límites de propiedad intelectual (Decreto Legislativo 822) y de seguridad nacional (Decreto Supremo 106-2017-PCM). Mediante el análisis del estándar regional de la Sentencia T-067 de Colombia, se concluye que la transparencia no es un concepto aislado, sino la evolución natural de la rendición de cuentas pública. Se propone la

* Doctoranda en Derecho Privado en la Universidad de Salamanca. Doctoranda en Educación en la Universidad de San Martín de Porres. Magíster en Derecho Empresarial por la Universidad de Lima. Magíster en Gerencia Social por la Pontificia Universidad Católica del Perú. Abogada por la Universidad de Lima. Docente de los cursos de Derechos Humanos y Derechos Fundamentales de la unidad de Virtualización Académica de la Universidad de San Martín de Porres. Jefa del Registro Nacional de Identificación y Estado Civil del Perú. Código ORCID: <https://orcid.org/0000-0002-2668-7774>

** Magíster en Derecho Empresarial por la Universidad de Lima. Magíster por la Universidad Autónoma de Madrid. Abogado por la Universidad de Lima. Consultor de empresas en áreas de derecho tributario, planeamiento tributario, revisiones contables-tributarias y derecho corporativo. Docente de Derecho Comercial I en la Facultad de Derecho de la Universidad de Lima y asesor del Círculo de Estudios de Derecho Comercial de dicha casa de estudios. Docente de Legislación Aduanera y Minera y de Auditoría Tributaria en la maestría en Ciencias Contables y Financieras de la Universidad de San Martín de Porres. Socio del Estudio Ramírez Abogados. Código ORCID: <https://orcid.org/0009-0008-9523-2125>

implementación de auditorías constantes y la supervisión humana para asegurar que la Administración pública algorítmica respete los derechos fundamentales y el control democrático.

PALABRAS CLAVE: transparencia algorítmica / inteligencia artificial / sesgo algorítmico / acceso a la información / Administración pública algorítmica

ALGORITHMIC TRANSPARENCY AS A DIMENSION OF THE RIGHT OF ACCESS TO INFORMATION

ABSTRACT. This article examines algorithmic transparency as a digital dimension of the right of access to public information in Peru. Faced with increasing state automation and the deployment of systems such as Curia and ElecclA, significant risks regarding the black box effect and biases that result in algorithmic discrimination have emerged. Drawing on the Political Constitution and the Inter-American precedent of *Claude Reyes v. Chile*, this research contends that explainability is vital for overseeing the State's technological power. The study approaches bias mitigation as a social justice objective, harmonizing it with legal limits such as intellectual property (Legislative Decree 822) and national security (Supreme Decree 106-2017-PCM). By analyzing the regional standard set by Colombia's Sentence T-067, it concludes that transparency represents a natural evolution of public accountability. Finally, it proposes the implementation of constant audits and human intervention to ensure that the algorithmic public administration remains subject to fundamental rights and democratic control.

KEYWORDS: algorithmic transparency / artificial intelligence / algorithmic bias / access to information / algorithmic public administration

1. INTRODUCCIÓN

La irrupción de la inteligencia artificial (IA) ha transformado la producción del conocimiento y toma de decisiones en el campo jurídico incorporándose a actividades judiciales y administrativas. Aunque se espera que la codificación sea neutral, los sistemas de IA son construcciones sociales y normativas basadas en el pensamiento humano previo, lo que permite que prejuicios y sesgos de sus programadores afecten los resultados finales. Esta evolución tecnológica ha transitado desde el *machine learning* y la inteligencia generativa —que dio origen a asistentes como ROSS o Harvey— hasta la actual IA agéntica, capaz de adoptar decisiones autónomas.

Sin embargo, esta potencia tecnológica conlleva daños sociales reales. Casos como el de Amazon —que evidenció sesgos de género— o SyRI en los Países Bajos —que mostró fallos en la detección de fraude basados en la racialización de personas— justifican la necesidad de la transparencia algorítmica como un derecho de defensa frente al Estado. En el Perú, la implementación de Curia (en el Poder Judicial) y ElecclA (en el Jurado Nacional de Elecciones) —sistemas de IA que apoyan proyectos de resolución de casos— plantea desafíos críticos: la opacidad o efecto de caja negra de estos algoritmos dificulta conocer los criterios de las decisiones automatizadas. En ese sentido, el poder tecnológico que otorgan al Estado debe ser un poder tecnológico fiscalizable para evitar la arbitrariedad en un entorno donde el poder estatal se vuelve invisible a través del *software*.

Por ello, la transparencia algorítmica no es solo una garantía técnica, sino la evolución natural del derecho de acceso a la información hacia un entorno digital. Así como anteriormente el ciudadano solicitaba expedientes físicos para controlar la Administración pública, hoy el ejercicio de ese mismo derecho exige acceder a la lógica de los algoritmos que emiten decisiones sobre sus derechos. En consecuencia, esta transparencia se configura como una dimensión digital del derecho de acceso a la información pública que permite el escrutinio democrático de lo que se denomina Administración pública algorítmica. Con ello, se busca evitar discriminaciones y asegurar la legitimidad estatal. Con lo dicho, el presente artículo intenta responder la siguiente pregunta: ¿cómo la incorporación de la transparencia algorítmica como dimensión del derecho de acceso a la información permite mitigar los sesgos en la toma de decisiones estatales en el Perú sin vulnerar la propiedad intelectual y la seguridad nacional?

El abordaje de esta pregunta plantea un doble desafío que constituye el eje central de este análisis. Por un lado, la mitigación de sesgos se establece como el objetivo de justicia social primordial para evitar que la automatización estatal replique desigualdades históricas (Simon et al., 2022). Por otro, el respeto a la propiedad intelectual y la seguridad nacional representan el reto de factibilidad jurídica que este estudio examina detalladamente analizando bajo qué condiciones el mandato de transparencia puede armonizarse con las restricciones del sistema peruano. Para ello, utilizaremos la doctrina

nacional e internacional, el estándar regional de la Sentencia T-067 de Colombia y el análisis de los límites normativos en el ordenamiento jurídico nacional.

El presente análisis se estructura en seis apartados que inician con esta introducción sobre el impacto de la IA y el planteamiento del problema. En segundo lugar, se desarrolla un marco teórico que fundamenta la transparencia como una extensión del derecho de acceso a la información según la Constitución peruana y la jurisprudencia interamericana. El tercer apartado aborda de manera conjunta la problemática del sesgo algorítmico y el control del poder tecnológico analizando los riesgos del efecto de caja negra frente a las facultades de explicabilidad y rendición de cuentas. Posteriormente, en la cuarta sección, se examina el estándar regional mediante la Sentencia T-067 de Colombia como modelo de éxito para el acceso al código fuente. El quinto apartado se centra en la factibilidad y los límites jurídicos en el Perú analizando la ponderación necesaria frente a la propiedad intelectual y la seguridad nacional. Finalmente, la sexta sección presenta las conclusiones que ratifican la necesidad de este derecho para asegurar que la tecnología esté al servicio de los derechos fundamentales y el control democrático.

2. CONCEPTOS CLAVE

2.1. El tratamiento del acceso a la información: referente interamericano

La transparencia algorítmica es una extensión del derecho de transparencia en general. En esa línea, el caso *Claude Reyes vs. Chile* grafica el acceso a la información como un derecho humano preexistente a nivel regional. Es decir, el principio de transparencia algorítmica en la Administración pública no constituye una prerrogativa jurídica emergente o aislada, sino una evolución directa y natural del derecho humano de acceso a la información.

Específicamente, el hito fundamental de esta doctrina se encuentra en la sentencia de la Corte Interamericana de Derechos Humanos (Corte IDH) para el caso *Claude Reyes y otros vs. Chile* (2006): el primer fallo internacional en reconocer explícitamente que el derecho a recibir información en manos del Estado está protegido de forma convencional bajo el artículo 13 de la Convención Americana sobre Derechos Humanos. Mediante el principio de máxima divulgación (*maximum disclosure*), la Corte IDH determinó que toda la información estatal se presume pública y que recae en el propio Estado la estricta carga de justificar y motivar de manera racional, proporcional y legal cualquier limitación o reserva.

El origen fáctico de dicho caso ilustra con precisión cómo la opacidad pública vulnera el control ciudadano: en 1998, un grupo de activistas ambientales solicitó al Comité de Inversiones Extranjeras de Chile datos sobre un megaproyecto de explotación forestal —el proyecto Cóndor— para evaluar su impacto ambiental y socioeconómico. El requerimiento

fue denegado por la autoridad alegando una supuesta reserva a terceros sin brindar fundamentación alguna. Al sancionar al Estado chileno por esta negativa arbitraria, la Corte IDH sentó un precedente definitivo: la Administración no puede escudarse en el secreto burocrático o el interés comercial corporativo para denegar información de alto impacto público. Trasladado este estándar al escenario tecnológico contemporáneo, se encuentra prohibido de forma tajante que las entidades públicas apelen a la complejidad técnica, la propiedad intelectual o el secreto comercial para ocultar el funcionamiento de los sistemas de IA empleados en la toma de decisiones.

2.2. Fundamentación nacional

En el ordenamiento jurídico peruano, la fundamentación nacional del derecho a la transparencia algorítmica se cimienta en el artículo 2, inciso 5, de la Constitución política, el cual consagra que toda persona tiene la facultad de solicitar, sin expresión de causa, la información que requiera y a recibirla de cualquier entidad pública en el plazo legal. Este derecho se constituye como un pilar fundamental del Estado democrático estableciendo un imperativo de transparencia que vincula a la Administración incluso cuando esta emplea herramientas de alta complejidad tecnológica.

Bajo este marco, se colige que la existencia de cajas negras tecnológicas en la gestión pública vulnera directamente el núcleo esencial de este derecho constitucional. Cuando el Estado peruano delega procesos críticos de forma automatizada —como la asignación de programas sociales, la evaluación de perfiles de riesgo o la fiscalización tributaria—, la ausencia de una debida motivación sobre el funcionamiento del código fuente o las variables ponderadas equivale jurídicamente a una denegación arbitraria de información. Por tanto, la opacidad algorítmica no puede ser amparada bajo criterios de modernización estatal, ya que la transparencia emerge como una dimensión obligatoria para garantizar la rendición de cuentas.

2.3. La transparencia algorítmica como dimensión digital

Bajo la premisa de que la transparencia algorítmica no constituye un derecho nuevo o inventado, su conceptualización se define como una extensión o evolución natural del derecho de acceso a la información hacia el entorno digital. Esta transición implica que el control ciudadano debe adaptarse a la realidad técnica actual, trasladando el foco del examen de expedientes y documentos físicos hacia la lógica de los sistemas y algoritmos que emiten decisiones con efectos jurídicos sobre los administrados. En este sentido, la transparencia se configura como una dimensión digital indispensable que permite el escrutinio de la Administración pública algorítmica y asegura que el mandato de apertura estatal se mantenga vigente frente a la automatización de la voluntad administrativa.

En esa medida, el acceso a la información algorítmica se constituye en un imperativo ético y jurídico que busca someter el poder tecnológico del Estado al escrutinio público y democrático. Al reconocer esta naturaleza evolutiva, se garantiza que el derecho de defensa y el principio de igualdad no queden anulados por la opacidad técnica. Asimismo, se busca que los ciudadanos no solo conozcan la existencia de un sistema, sino que comprendan los criterios que rigen las decisiones que afectan su autonomía personal.

3. PROBLEMÁTICA DEL SESGO Y EL CONTROL DEL PODER TECNOLÓGICO

3.1. El sesgo algorítmico como riesgo jurídico y social

La tecnología no es neutral y sí puede afectar los derechos fundamentales. En principio, los sistemas de IA no son objetivos, sino construcciones sociales que incorporan prejuicios humanos desde su diseño y entrenamiento. El sesgo algorítmico está referido a la situación en que un sistema automatizado —como la IA— produce resultados desfavorables para una persona o determinados grupos de personas estableciendo escenarios de segregación o discriminación. Es decir, el sistema adopta decisiones que perjudican a los individuos por razones de raza, género, etnia, edad, discapacidad, nivel socioeconómico, entre otros. Recordemos el caso de la empresa Amazon que deshabilitó su sistema de IA para contratación de personal, ya que la aplicación prefería contratar hombres antes que mujeres.

El sesgo se manifiesta como errores o diferencias de desempeño del sistema: por ejemplo, con falsos positivos o falsos negativos, esto es, cuando el sistema afirma “sí” cuando debió negar o separar algún dato, o cuando indica “no” cuando debió afirmar o incluir alguna información. Así, el sistema genera tratamientos diferenciados a partir de datos históricos con desigualdades incorporadas y reglas de decisión que expresan, directa o indirectamente, elecciones humanas.

El sesgo algorítmico es conocido también como discriminación algorítmica cuando las diferencias se traducen en una desigualdad jurídicamente relevante. En inglés, esta problemática es conocida como *machine bias*, pues vincula las exclusiones con decisiones automatizadas en temas sensibles como la justicia, el empleo o el crédito. Para la elaboración de *software* o aplicativos informáticos, suele identificarse un proceso básico: entradas, procesamiento y salidas. En este circuito, los estudios ubican diversas fuentes del sesgo como puntos críticos en los que se incorporan prejuicios o se reproducen desigualdades. Así, los sesgos se pueden presentar de la siguiente manera:

- a) Sesgo en la especificación del problema. El programador —el ser humano— define categorías como mérito, riesgo, fraude o éxito. La forma de conceptualizarlas, operativizarlas y convertirlas en variables del sistema

puede perjudicar a ciertos grupos sociales. Por ejemplo, no considerar a personas rehabilitadas luego de cumplir su pena privativa de libertad por tales antecedentes.

- b) Sesgo en los datos de entrenamiento. Conjuntos no representativos o cruzados por desigualdades históricas producen modelos que replican esas mismas desigualdades. Por ejemplo, si los datos presuponen que las personas con discapacidad rinden menos, el sistema puede reducir sus posibilidades en procesos automatizados de selección laboral.
- c) Sesgo por selección de variables (*proxies*). Se alimenta al sistema con variables aparentemente neutrales que, en la práctica, se correlacionan con atributos protegidos. Por ejemplo, usar historial de consumo o lugar de vivienda como sustituto de etnia o clase social generan un trato desigual.
- d) Sesgo por transferencia de contexto. El modelo se desarrolla para un entorno cultural y social determinado, pero se aplica en otro distinto en el que las costumbres son diferentes. Esto explica el riesgo de importar *software* construido para una realidad ajena y desplegarlo en el Perú. El sistema puede producir discriminaciones no intencionadas por un desajuste cultural, institucional o lingüístico, características que no fueron consideradas en su programación original adaptada a otra realidad.
- e) Sesgos humanos incorporados y sesgos estadísticos. El sistema reflejará valores y sesgos de quienes codifican, programan y de quienes recolectan los datos; por ello, la selección del equipo técnico y la supervisión del ciclo de vida del sistema son determinantes. No obstante, pretender una neutralidad total es insuficiente; el punto crítico es diseñar mecanismos de control, auditorías, explicabilidad y correcciones. Los sistemas informáticos, sobre todo con uso de IA, deben ser auditados constantemente para lograr actualizaciones de mejora.

Desde una perspectiva de protección jurídica, el debate no se reduce a abrir el sistema en sentido absoluto (desagregar su código fuente). En materia de derecho de acceso a la información para lograr la explicabilidad del funcionamiento de la IA u otra aplicación informática, se ha sostenido que “el derecho a la información no implica que se deba abrir el *black box*” (Morales Cáceres, 2021, p. 66); más bien, el estándar exigible debe orientarse a que el titular pueda comprender por qué se tomó una decisión determinada y no otra, y conocer cómo oponerse a ella incluyendo la posibilidad de solicitar intervención humana (p. 66).

En este marco, la doctrina ha planteado instrumentos concretos para evitar que el sesgo se mantenga invisible. Se ha propuesto, por ejemplo, la implantación de estudios de

impacto algorítmico semejantes a los de impacto ambiental o de género, pues el impacto algorítmico puede coincidir con el de género y debería integrarse en él (Rivas Vallejo, 2021). Además, se advierte que, aunque la transparencia intervenga como criterio en el sector público, en el ámbito privado se presentan límites como la propiedad intelectual (derechos de autor), el secreto industrial o la lógica competitiva (confidencialidad de la información) (Rivas Vallejo, 2021).

Existen casos emblemáticos de sesgo algorítmico como el Computation Offender Management Profiling for Alternative Sanctions, un *software* utilizado en los Estados Unidos para predecir la posibilidad de reincidencia de una persona que antes había sido sentenciada. El dictamen algorítmico se usaba en decisiones judiciales y de finanzas; sin embargo, se descubrió que el sistema etiquetaba erróneamente a personas de tez negra con el doble de probabilidad de reincidencia, mientras que las personas de tez blanca eran rotuladas con una menor reincidencia, aunque antes hubieran cometido delitos mucho más graves.

El estudio Gender Shades, de herramientas de reconocimiento facial, demostró cómo sistemas de empresas como IBM o Microsoft, al momento de reconocer a personas por su género y color de piel, presentaban altas tasas de error para los casos de mujeres con piel oscura, mientras que el error era mínimo en el reconocimiento facial de hombres blancos. En la misma línea, el sistema SyRI de los Países Bajos, empleado para detectar fraude en prestaciones sociales, fue invalidado judicialmente en el 2020 al comprobarse que perfilaba desproporcionadamente a residentes de barrios de bajos ingresos y de origen migrante.

Pero los casos de sesgos algorítmicos no son recientes. El caso Da Cunha contra Yahoo de Argentina y Google, del 2009, mostró cómo la configuración, programación o digitación humanas conllevan a incorporar determinadas categorías que relacionan indebidamente a las personas. Este caso reflejó cómo los motores de búsqueda utilizaban el sesgo en su dimensión asociativa (vinculación automatizada de nombres con ciertas categorías o contenidos). La demandante —modelo, cantante y actriz— reclamó el cese del uso no autorizado de su nombre e imagen con la correspondiente indemnización por daños y perjuicios a su imagen. Sostuvo que, al buscar su nombre en Yahoo y en Google, aparecían enlaces e imágenes vinculadas a contenidos sexualizados, eróticos o pornográficos sin su consentimiento y en contradicción con su trayectoria profesional.

La pericia informática solicitada por el juzgador explicó el funcionamiento de los buscadores. Se resaltó que los motores de búsqueda en internet comparan la palabra preguntada por el usuario con un archivo índice de datos procesados previamente para luego publicar los resultados de acuerdo con los criterios preestablecidos por mano humana en cada buscador (Juzgado Nacional en lo Civil, 2009). La pericia fue decisiva para demostrar que sí existía capacidad técnica de intervención por parte de los motores

de búsqueda demandados, pues sí era técnicamente factible evitar determinadas vinculaciones: “Es posible establecer filtros estáticos que no permitan indexar sitios” (Juzgado Nacional en lo Civil, 2009, p. 7) con contenidos pornográficos o “establecer otros que no permitan indexar imágenes de determinadas personas” (p. 7). La pericia también explicó el papel de los *metatags*: etiquetas invisibles para el visitante común que pueden ser usadas para atraer tráfico mediante palabras muy utilizadas, lo que incrementa la probabilidad de asociaciones engañosas (Juzgado Nacional en lo Civil, 2009). Desde la teoría del sesgo, este caso refuerza la tesis central: el buscador no crea el contenido, pero sí lo organiza, lo prioriza y lo asocia, produciendo efectos jurídicamente relevantes.

Otro caso judicial que muestra cómo la configuración de las aplicaciones conlleva a discriminaciones, prejuicios o sesgos es el caso de Costeja González contra Google Spain (Tribunal de Justicia de la Unión Europea [TJUE], 2014). Este promovió el control normativo sobre los efectos del algoritmo de búsqueda al reconocer que la indexación automatizada podía afectar derechos fundamentales. En este caso, Mario Costeja González presentó una reclamación ante la Agencia Española de Protección de Datos (AEPD) señalando que, al introducir su nombre en el buscador Google, aparecían enlaces a una publicación del diario *La Vanguardia* de 1998. La publicación trataba sobre un embargo por deudas a la Seguridad Social que ya había sido resuelto hacía muchos años. Costeja González solicitó que el periódico eliminara o modificara la publicación y que Google suprimiera los enlaces de su índice de resultados relacionados a tal información, ya que carecía de relevancia actual.

La AEPD rechazó la solicitud contra el periódico al considerar que la publicación era legal, pero la admitió con relación a Google. Consideró que el motor de búsqueda sí realizaba un tratamiento de datos personales, lo que fue confirmado por el TJUE, el cual estableció que la actividad consistente en rastrear información publicada por terceros, indexarla automáticamente, almacenarla temporalmente y ponerla a disposición de los usuarios según un determinado orden de preferencia sí constituía un tratamiento de datos personales. Es decir, el buscador se convierte en un agente que organiza, jerarquiza y presenta la información según criterios algorítmicos propios dependientes de la programación con la cual ha sido elaborado.

Al respecto, el TJUE permite al demandante ejercer su derecho a solicitar la eliminación de enlaces cuando la información resulte inadecuada, no pertinente o excesiva, sobre todo si ha transcurrido un periodo de tiempo prudencial y no existe un interés público que justifique mantenerla en línea. Esta disposición ha sido conocida como el derecho al olvido. Cabe destacar respecto a este caso que el Tribunal reconoció que la indexación por nombre propio permite construir una visión estructurada del individuo, lo que puede ampliar determinados hechos pasados y afectar desproporcionadamente la vida privada del sujeto. Es decir, se comprueba que el algoritmo de búsqueda determina

qué información aparece, en qué orden y con qué grado de visibilidad, de modo que sí genera un impacto cualitativamente distinto al de la publicación original.

Todos los casos revisados refuerzan la necesidad de incluir el derecho a la transparencia algorítmica como medida de control, auditorías y explicabilidad del funcionamiento de cada algoritmo, *software* o aplicación que conlleve a una decisión o a efectos sobre la persona.

3.2. La opacidad de la caja negra y el poder tecnológico

La opacidad y la transparencia son elementos fuertemente relacionados. La opacidad algorítmica se refiere a la falta de elementos suficientes para conocer cómo operan los algoritmos o cómo llegan a sus resultados (Garrido et al., 2021). La opacidad podría basarse, en principio, en la intención de quienes desarrollan o implementan el algoritmo (Mittelstadt et al., 2016), pero también podría estar basada en un limitado conocimiento de los receptores de la información, puesto que es una labor de especialistas y no siempre incluyen la experiencia del receptor o usuario. Además, la opacidad podría deberse a situaciones propias del lenguaje matemático en el que se basan y desarrollan los algoritmos.

Se relaciona también con la idea de opacidad el término *caja negra* (*black box*), entendida como la dificultad o imposibilidad de explicar cómo el sistema llega a un resultado. Si un programa de IA arrib a un resultado sin ninguna explicación, ello conduce a la pregunta: ¿cómo justificar decisiones que ni siquiera sus propios desarrolladores pueden reconstruir plenamente? Como señala Morales Cáceres, “a esto se le denomina *black box* o ‘caja negra’” (2021, p. 66). La opacidad o secretismo de los algoritmos dificulta conocer los criterios que han sido utilizados para arribar a decisiones automatizadas, lo que puede afectar el derecho de defensa, el principio de igualdad y no discriminación, el derecho a ser juzgado por seres humanos y dañar la legitimidad estatal.

Más adelante, veremos un caso emblemático colombiano que proyecta jurisprudencia y elementos que fortalecen la justificación de la necesidad de control del poder tecnológico. Ello mediante el reconocimiento expreso del derecho a la transparencia algorítmica y la precisión de que la complejidad técnica de los algoritmos no puede justificar su opacidad ni limitar el control ciudadano como parte del derecho de acceso a la información pública (Corte Constitucional de Colombia, 2025).

En esa línea lógica, se hace necesario plantear la noción de poder tecnológico. Esta noción define la capacidad del Estado para ejercer autoridad mediante el *software*; más aún, ejercer autoridad, clasificar y decidir sobre los ciudadanos mediante algoritmos opacos que eluden los controles democráticos tradicionales. Esta idea está adherida a la propia noción de poder del Estado, el cual tiene instrumentos que le sostienen como la carta magna

donde se plasman los derechos y deberes de los ciudadanos. Así, el poder tecnológico está encarnado en el propio poder del Estado. En ese sentido, Weber (1922/2014) señala que el Estado concentra el mayor poder dentro de la sociedad, condición necesaria para que pueda existir el orden social. La sociedad le cede ese poder al Estado para que actúe como la última muralla contra el caos. Sin embargo, ese poder solo es legítimo si descansa en una justificación ética derivada del pacto social (Rousseau, 1762/2017). En consecuencia, el Estado solo puede ejercer legítimamente ese poder cuando lo orienta a proteger la libertad de todos y busca el bien común del que él mismo forma parte.

En esa línea, es enteramente aceptable que el poder del Estado implique el poder tecnológico por el cual el mismo Estado implanta acciones basadas en lenguaje de IA y algoritmos. Ello no desvirtúa los deberes y principios del poder del Estado, sino que los ordena o justifica. Por tanto, el poder tecnológico le compete al Estado y este no puede escapar de los principios de ese poder, el cual debe saber administrar a favor de los ciudadanos, lo cual incluye la transparencia algorítmica.

3.3. Las dimensiones de la transparencia como mecanismos de control

La transparencia no es un fin en sí mismo, sino una importante herramienta para mitigar los riesgos antes expuestos: “abrir el código” y lograr que el ciudadano comprenda el porqué de una decisión. La transparencia implica dos facultades para controlar el poder. En primer lugar, el acceso, que se evidencia en conocer la existencia de la IA y los datos utilizados. En segundo lugar, la explicabilidad, que busca que el ciudadano comprenda el porqué de una decisión; es decir, no solo que acceda a la información sino, centralmente, que esta información sea clara.

Es así como la transparencia algorítmica no se limita a la publicación del código fuente, sino que implica la posibilidad de comprender el funcionamiento del sistema y los criterios utilizados en la toma de decisiones (Delva Benavides & Mendez Gonzalez, 2025). Ello resulta esencial ya que muchos sistemas de IA operan como cajas negras, lo que dificulta su comprensión por parte de los ciudadanos. En ese sentido, el derecho a la transparencia algorítmica se define como la facultad de los individuos de acceder a la información sobre el funcionamiento, la lógica, los criterios y los efectos de los sistemas automatizados que inciden en sus derechos, información que debe brindarse de manera accesible y comprensible (Abad Alcalá, 2026).

Por tanto, la transparencia algorítmica constituye la divulgación de información suficiente sobre los sistemas informáticos para facilitar su supervisión, evaluación e, incluso, eventual impugnación; sobre todo si afectan derechos fundamentales (Pauner Chulvi, 2023). Ello resulta particularmente relevante en la medida en que las personas pueden ser evaluadas, clasificadas o incluso sancionadas mediante sistemas automatizados sin que se conozcan los criterios utilizados para adoptar dichas

decisiones. Como advierte la doctrina, no es posible garantizar la legitimidad de las decisiones automatizadas ni el respeto de los derechos fundamentales sin que estas sean sometidas al escrutinio público y democrático (Concha Camacho, 2024). En otras palabras, sin que sean sometidos a procesos de transparencia.

Desde el punto de vista jurídico, el derecho a la transparencia algorítmica se constituye en una extensión del derecho de acceso a la información pública. Este es considerado uno de los pilares del Estado democrático y se ha hecho evidente en el nuevo contexto en el que el uso de la IA es constante. El derecho a la transparencia permite a los ciudadanos conocer cómo el Estado adopta decisiones automatizadas que afectan sus derechos (Bonnet Parejo, 2025) y, además, garantiza la autonomía personal y el control democrático del poder tecnológico (Concha Camacho, 2024).

Es por ello que se sostiene que la transparencia algorítmica constituye una garantía frente al ejercicio arbitrario del poder estatal, pues permite el control jurídico de las decisiones automatizadas. Ello incluye el acceso a sus criterios de funcionamiento, su lógica y programación y, con ello, al código fuente, de modo que los ciudadanos pueden auditar los algoritmos y verificar que no contengan sesgos o discriminaciones indebidas (Bonnet Parejo, 2025). Así visto, la transparencia algorítmica es más que un principio técnico: se constituye en un estándar jurídico que limita el poder tecnológico del Estado y de las grandes plataformas digitales. La doctrina señala que la transparencia algorítmica se instaure como un mecanismo fundamental de rendición de cuentas al permitir controlar las decisiones automatizadas y garantizar el respeto de los derechos fundamentales (Abad Alcalá, 2026). Con ello, se asegura que las decisiones automatizadas sean comprensibles, explicables y controlables por la ciudadanía.

La doctrina ha identificado diversas dimensiones del derecho a la transparencia algorítmica. Por ejemplo, comprende el derecho de acceso a la información algorítmica, que implica el derecho a conocer la existencia del algoritmo, su finalidad, los datos utilizados y los criterios de decisión aplicados (Bonnet Parejo, 2025); ello porque es importante conocer qué parte del proceso incluye aplicaciones informáticas, uso de IA, procesamiento digital y tecnología en general. De otro lado, la transparencia algorítmica comprende el derecho al control y a la rendición de cuentas, ya que ayuda a evaluar si las decisiones automatizadas respetan los derechos fundamentales. Actualmente, se aplica en la Administración pública ayudando a los administrados a controlar los algoritmos usados por el Estado. Destacamos los casos emblemáticos expuestos anteriormente que demuestran que los algoritmos pueden afectar derechos como el acceso al empleo, los beneficios sociales o la libertad personal, por lo que resulta indispensable garantizar su control jurídico (Abad Alcalá, 2026).

Un caso destacable sobre derecho al control y rendición de cuentas lo configura el caso Bosco de España. En este, un grupo de ciudadanos denunciaron sesgos en Bosco,

un *software* utilizado por la Administración estatal española para otorgar un bono social eléctrico. La denuncia ocurrió tras detectar constantes denegaciones injustificadas en el otorgamiento del bono. El Gobierno se negó a otorgar el código fuente del *software* bajo los sustentos de que este era protegido por la propiedad intelectual, además de no poder otorgarse por cuestiones de seguridad nacional. Sin embargo, el Tribunal Supremo reconoció el derecho ciudadano a acceder al algoritmo utilizado por la Administración pública destacando que no pueden existir cajas negras en el ámbito tecnológico cuando estas herramientas son utilizadas para la toma de decisiones automatizadas. Ello, en consideración del principio de transparencia algorítmica (Bonnet Parejo, 2025).

Este derecho se aplica, asimismo, en el ámbito de las plataformas digitales, las cuales utilizan algoritmos para seleccionar contenidos, dirigir publicidad y organizar la información. Como se ha revisado, los algoritmos pueden afectar derechos fundamentales como la libertad de expresión y la privacidad, lo que hace necesaria su transparencia (Pauner Chulvi, 2023). Sin embargo, el derecho a la transparencia algorítmica presenta también conflictos con otros derechos, sobre todo, con la protección de datos personales y los secretos comerciales, ya que las empresas suelen negarse a revelar sus algoritmos alegando protección de su propiedad intelectual. Con actitudes como esa, se enfrentan al deber de transparencia y la protección de intereses económicos (Delva Benavides & Mendez Gonzalez, 2025).

4. LA SENTENCIA T-067 DE COLOMBIA COMO REFERENTE REGIONAL SOBRE EL DERECHO A LA TRANSPARENCIA ALGORÍTMICA

Colombia ofrece una de las experiencias más relevantes para otros países: su Corte Constitucional ordenó la entrega del código fuente de una aplicación estatal al considerarlo un protocolo digital de actuación administrativa. La Corte Constitucional de Colombia ha sido pionera en reconocer el derecho a la transparencia algorítmica en su Sentencia T-067 del 2025 (Exp. T-8.202.533). En esta, declaró fundada una acción de tutela (símil de la acción de amparo en el Perú) interpuesta por el ciudadano Juan Carlos Upegui Mejía, quien consideró vulnerado su derecho de acceso a la información pública. La Corte Constitucional ordenó la entrega del código fuente de la aplicación estatal CoronaApp, la que posteriormente fue trasladada a otra entidad y funcionó bajo el nuevo nombre de Mi Salud Digital. La Corte sostuvo que el acceso al código fuente sí constituía una manifestación del derecho fundamental de acceso a la información pública en su vertiente de transparencia algorítmica por parte de la Administración estatal (Corte Constitucional de Colombia, 2025).

El 6 de agosto del 2020, el demandante presentó una petición ante la Agencia Nacional Digital en la que solicitaba copia del código fuente del aplicativo CoronaApp, incluyendo sus versiones y registros históricos. CoronaApp fue el aplicativo elaborado por el Gobierno

colombiano para medir las estadísticas e impacto del coronavirus durante la pandemia por COVID-19. Para ello, utilizó información ciudadana con especial énfasis en datos médicos. Upegui Mejía sostuvo que el código fuente¹ constituía información pública relacionada con una herramienta estatal usada como instrumento de política pública durante la pandemia de COVID-19, ya que había sido elaborado con recursos públicos. Destacó que el código fuente no contenía datos personales, ya que solo se trataba de instrucciones de programación, las cuales se equiparan a un protocolo digital de actuación administrativa que indica cómo va a funcionar y procesar la información el aplicativo. Añadió que su pedido permitiría el control ciudadano sobre una herramienta estatal que procesaba datos personales de millones de ciudadanos colombianos. Toda esta fundamentación se basó en la Ley 1712 del 2014, norma relacionada al derecho de acceso a la información pública en Colombia.

La Agencia Nacional Digital negó el pedido sustentando que el acceso al código fuente pondría en riesgo la privacidad y la seguridad de los datos personales de los ciudadanos, ya que posibilitaría ataques informáticos, clonación de la aplicación y otras formas de explotación de posibles vulnerabilidades del sistema. Añadió en su argumento que el *software* se encontraba aún en fase de desarrollo y que el código fuente estaba protegido por los derechos de autor, cuyo titular era el Instituto Nacional de Salud. Al ser consultado el Ministerio de Salud para la entrega del código fuente, este sostuvo que no podría entregarlo ya que este constituía un activo crítico desde la perspectiva de la seguridad de la información y que su difusión comprometería la integridad de la plataforma y la protección de los datos personales.

Considerando estos argumentos, las instancias judiciales negaron la acción de tutela, pues admitieron como razonable mantener el código fuente en reserva para proteger la seguridad de la información, la seguridad pública, los derechos de autor y evitar la afectación del derecho a la intimidad de los usuarios. Las decisiones se basaron en las excepciones al derecho de acceso a la información previstas en la Ley 1712 del 2014. No obstante, el demandante insistió en sus argumentos y añadió que, si hubiese datos personales, podría hacerse una divulgación parcial del código fuente entregando la información que no tuviera relación con tales datos. También sustentó que las autoridades no habrían aplicado el test de daño exigido por la Ley 1712, examen que permite demostrar que la difusión de la información sí causaría un daño presente, probable y específico.

La Corte concluyó que las entidades demandadas solo se habían limitado a invocar riesgos genéricos sin demostrar la existencia de un daño concreto: “Las autoridades accionadas no demostraron de manera específica, clara y suficiente el daño que podría

1 Un código fuente se entiende como el conjunto de comandos e instrucciones que los programadores informáticos utilizan, mediante lenguaje de programación, para el funcionamiento de un *software*, aplicación informática o sitio web.

derivarse de la divulgación del código fuente, ni explicaron por qué dicho daño superaría el interés público en conocer esta información” (Corte Constitucional de Colombia, 2025, párr. 112). Asimismo, la Corte determinó que la protección de los derechos de autor no constituye por sí misma una causal suficiente para negar el acceso a información pública: “El hecho de que el código fuente esté protegido por derechos de autor no implica que se trate de información reservada, ni excluye la aplicación del derecho fundamental de acceso a la información pública” (párr. 118).

Uno de los aportes más importantes de la sentencia es el reconocimiento expreso del derecho a la transparencia algorítmica, al cual la Corte definió como “el conjunto de obligaciones estatales encaminadas a garantizar que la ciudadanía pueda conocer, comprender y auditar los sistemas algorítmicos utilizados por el Estado” (Corte Constitucional de Colombia, 2025, párr. 124). Asimismo, señaló que la complejidad técnica de los algoritmos no puede justificar su opacidad, pues “la complejidad técnica de los algoritmos no puede convertirse en una barrera para el control ciudadano ni en un obstáculo para el ejercicio del derecho fundamental de acceso a la información pública” (párr. 126).

Para la Corte, “la transparencia algorítmica es un componente esencial del principio democrático y de la rendición de cuentas en el Estado constitucional” (Corte Constitucional de Colombia, 2025, párr. 129). Por tanto, se revocaron las decisiones judiciales previas y se ordenó entregar el código fuente al demandante. También se ordenó al Estado colombiano adoptar medidas para fortalecer la transparencia algorítmica señalando que “las entidades públicas deben implementar mecanismos que garanticen la transparencia de los sistemas algorítmicos utilizados en la toma de decisiones públicas” (párr. 133).

5. FACTIBILIDAD Y LÍMITES JURÍDICOS DE LA TRANSPARENCIA ALGORÍTMICA EN EL PERÚ

En el Perú, las principales excepciones para la transparencia algorítmica están vinculadas con la seguridad y la protección de datos personales. En ese sentido, el Decreto Supremo 106-2017-PCM restringe la transparencia en casos de seguridad nacional extrema debidamente motivados; asimismo, el Decreto Legislativo 822, que regula el derecho de autor, y la Ley 29733, que establece el régimen de protección de datos personales. Debe incorporarse mecanismos de supervisión para un mejor control de las aplicaciones informáticas. En ese sentido, se requiere la implementación de auditorías y de una supervisión constante, como en el caso de procesos de revisión periódica, para poder asegurar que los algoritmos sigan siendo justos y no discriminatorios.

Si bien el reto pasa por actualizar todas esas normatividades a una sociedad que respete la inclusión, es necesario tener en cuenta ciertas pautas para decidir la entrega o

no de los códigos fuente como base de la transparencia algorítmica. Así, se debe evaluar lo siguiente:

- a) El código fuente es distinto a los datos personales y no debe tener relación con los mismos

Al tratarse de instrucciones de programación que determinan cómo funcionará el sistema informático, el código fuente no incluye datos personales. Podría ocurrir que —al momento de hacer pruebas sobre cómo funciona el aplicativo en su fase de recolección de datos, interoperabilidad con base de datos personales o fase de procesamiento de tales datos— se utilicen datos personales; sin embargo, para ello, se recomienda usar datos ficticios o anonimizar los datos usados. Luego de las pruebas, tal información debe ser borrada o criptografiada para asegurar su no acceso. Así, el código fuente a entregar solo incluirá las reglas del proceso y ningún dato personal.

De otro lado, si la elaboración del *software* incluye la interoperabilidad con alguna base de datos que contenga datos personales, debemos precisar que son dos aplicaciones distintas; uno es el sistema informático principal, seguido de la aplicación secundaria, que es la base de datos. Ambas se interconectan para que el sistema principal obtenga datos de la aplicación secundaria, pero el *software* complementario tiene su propio código fuente, distinto al código fuente del sistema principal. El código fuente del primer sistema tendrá como parte de sus instrucciones el conectarse a la base de datos y las indicaciones de qué hacer luego de obtener o no la información esperada. En todo caso, los datos personales obtenidos no son parte del código fuente, sino del banco de datos o almacén de datos del *software* principal.

- b) La protección del código fuente por los derechos de autor vs. la transparencia algorítmica

Todo programa de ordenador, *software*, aplicativo informático o base de datos informática está protegida por derechos de autor. De acuerdo con la ley peruana sobre el derecho de autor, Decreto Legislativo 822, los programas de ordenador y bases de datos están protegidas por el derecho de autor y son inscribibles ante el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi). El registro es declarativo, pero inscribir los programas informáticos ayuda a dar mayor protección jurídica. Para el registro, se presenta la obra en sí, más el código fuente, el manual de usuario y demás documentación que acredite el funcionamiento del *software*. La ley de derecho de autor precisa que las bases de datos también son inscribibles considerando su estructura, pero no los datos que alberga.

En el caso de la Administración pública que encarga el desarrollo de un sistema informático, el contrato debe establecer claramente que el titular de los derechos patrimoniales del autor es la entidad que encargó el desarrollo, por lo que podrá hacer entrega del código fuente. En otros casos, el *software* es elaborado por el personal de la Oficina de Tecnologías de la Información de la institución, por lo que la Administración pública bien puede entregar el código fuente.

Si el programa informático contiene *software* propietario en su desarrollo, es decir, aquel que es pagado, entonces deberá evaluarse que no podrá entregarse un código fuente de un *software* cuya autoría ni cesión es estatal. No obstante, en algunos casos, la Administración pública desarrolla sus aplicaciones informáticas utilizando *software* libre, aquel que, más allá de no solicitar un pago por su uso, permite el empleo libre del código fuente, el cual es conocido y está en abierta disposición. Tal información sí puede ser entregada como parte del código fuente del aplicativo informático estatal.

Finalmente, debe tenerse en cuenta que la elaboración de las aplicaciones informáticas de las entidades del Estado se realiza utilizando presupuesto público tanto en el pago de la contratación de los desarrolladores como en la contratación del propio personal informático, la adquisición de *software* propietario, uso de *software* libre, uso de nubes para el desarrollo informático, entre otros. Por tanto, todo sistema informático está sometido a las normas de acceso a la información pública y a la transparencia algorítmica, de modo que los derechos de autor ceden ante la necesidad de transparencia pública.

c) La culminación o no de un *software* vs. la transparencia algorítmica

Uno de los sustentos para negar el otorgamiento del código fuente en la sentencia colombiana apuntó a que el aplicativo informático se encontraba en desarrollo y, por tanto, al no estar culminado, no podía entregarse el código fuente. Ante ello, debe entenderse qué significa una aplicación en desarrollo, término que puede aplicarse cuando el *software* o sistema informático está siendo elaborado, es decir, el código fuente está aún en construcción. Cuando se culmina la aplicación, esta ingresa a una fase de prueba o marcha blanca que permite evaluar su funcionamiento (por ejemplo, si cumple el objetivo, si se detectan fallas, etcétera). Superada la fase de marcha blanca, se pone el aplicativo en producción, lo que significa que está culminado para la operatividad.

Por supuesto que un sistema informático requiere mejoras y actualizaciones de acuerdo con los casos que se vayan encontrando, las modificaciones legales que se aprueben o las actualizaciones informáticas que aparezcan posteriormente. Ningún elemento tecnológico deja de modernizarse, pues

las características de la sociedad digital son justamente el dinamismo, la mejora continua y la búsqueda de la mayor funcionalidad y comodidad para los usuarios. Por tanto, si una aplicación informática es lanzada y utilizada públicamente, se le considera culminada, por lo que el código fuente puede ser entregado.

d) La seguridad o constitución de activo crítico como protector del código fuente

El código fuente debe ser evaluado de acuerdo con las características y uso de las aplicaciones informáticas. No es lo mismo una aplicación que genera estadísticas poblacionales que una aplicación que ayuda a conocer el buen funcionamiento de las estaciones base y antenas de telecomunicaciones. La primera ayuda a la academia y a la toma de decisiones para políticas públicas; la segunda contribuye a mantener al país comunicado monitoreando y evitando problemáticas o posibles ataques que afecten el funcionamiento, así como una actuación para su rápida reposición.

Esto significa que la entrega del código fuente debe evaluarse bajo un contexto de seguridad ciudadana de apoyo a la confidencialidad de la información o secreto de Estado. Actualmente, el Perú cuenta con el Decreto Supremo 106-2017-PCM, norma que aprueba el Reglamento para la identificación, evaluación y gestión de riesgos de los activos críticos nacionales (ACN), en cuyo fundamento se señala lo siguiente:

Que, los activos críticos nacionales (ACN) son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales;

Que, la afectación, perturbación o destrucción de los ACN no permite soluciones alternativas inmediatas, generando grave perjuicio a la nación. Por dicha razón, es necesario establecer, mediante normativa especial, los criterios que deben observar, a nivel nacional, los sectores responsables, las entidades públicas y las empresas privadas, para gestionar la protección y seguridad de los ACN.

Será importante evaluar si la entidad pública se ha constituido como ACN, ya que ello podría ser causal para postergar o limitar la entrega del código fuente y, por tanto, limitar el derecho a la transparencia algorítmica. Por ello, también es vital que los programadores informáticos cuiden, en la elaboración de las aplicaciones, la seguridad de la información y cualquier tipo de riesgo posible a un ataque informático. En ese sentido, el *software* debe estar muy bien elaborado, no solo desde el punto de vista de la funcionalidad, sino también desde la mirada de la seguridad.

- e) La debida motivación es base ante la negativa de la transparencia algorítmica

Finalmente, el deber de motivación, principio básico del derecho administrativo y del derecho procesal, es vital, sobre todo ante la denegación del derecho a la transparencia algorítmica. La ciudadanía debe comprender los motivos y fundamentos por los cuales no puede acceder a un algoritmo o código fuente, y tales sustentos deben implicar un análisis de riesgos, de proporcionalidad de derechos y de posibles daños utilizando un lenguaje comprensible.

Asimismo, será pertinente motivar debidamente la procedencia de los pedidos de transparencia algorítmica no solo por principio, sino también para lograr un mayor y sustentado desarrollo de este nuevo derecho.

6. CONCLUSIONES: HACIA UNA JUSTICIA ALGORÍTMICA EN EL PERÚ

Se concluye que la transparencia algorítmica no constituye un derecho emergente o aislado, sino que es la evolución natural y una dimensión digital indispensable del derecho fundamental de acceso a la información pública, consagrado en el artículo 2, inciso 5, de la Constitución política del Perú. Esta interpretación permite que el control ciudadano se desplace del examen de expedientes físicos hacia la auditoría de la lógica y los criterios de los sistemas que rigen la Administración pública algorítmica.

La incorporación de este derecho es el instrumento jurídico primordial para mitigar los sesgos algorítmicos (de especificación, datos, *proxies* o transferencia de contexto) que pueden derivar en discriminación algorítmica. Al garantizar las facultades de acceso, explicabilidad y rendición de cuentas, el Estado peruano asegura que las decisiones automatizadas no repliquen desigualdades históricas y permite que la tecnología esté al servicio de la autonomía personal y no del ejercicio arbitrario del poder tecnológico.

El análisis demuestra que la protección de la propiedad intelectual (Decreto Legislativo 822) no es una causal absoluta para el secretismo estatal. Dado que el *software* público se desarrolla con presupuesto estatal, los derechos de autor deben ceder ante el mandato de transparencia pudiendo el Estado entregar el código fuente (entendido como un protocolo digital de actuación administrativa) sin afectar intereses comerciales privados.

Respecto de la seguridad nacional y los ACN (Decreto Supremo 106-2017-PCM), se establece que estos límites deben aplicarse bajo un test de daño estricto. El Estado no puede invocar riesgos genéricos para negar información: cualquier reserva debe estar debidamente motivada —demostrando un daño presente, específico y probable— y debe permitir, en última instancia, el uso de técnicas como la anonimización o datos ficticios para garantizar la fiscalización sin comprometer la infraestructura.

Finalmente, la transparencia algorítmica en el Perú exige pasar de una fiscalización reactiva a una supervisión proactiva y constante. Esto implica implementar auditorías periódicas y estudios de impacto algorítmico que aseguren la explicabilidad jurídica (entender el porqué de la decisión) por encima del simple acceso técnico. Con ello se debe garantizar el derecho de los ciudadanos a solicitar la intervención humana ante resultados automatizados injustos.

REFERENCIAS

- Abad Alcalá, L. (2026). Transparencia algorítmica: enfoques y desafíos para el Estado democrático. *Revista Española de la Transparencia*, (23), 91-138. <https://doi.org/10.51915/ret.443>
- Bonnet Parejo, M. (2025). El principio de transparencia algorítmica en el derecho público español. *Revista Canaria de Administración Pública*, (6), 263-281. <https://doi.org/10.36151/RCAP.6.9>
- Concha Camacho, W. (2024). El derecho a la transparencia algorítmica como estándar ético en una democracia liberal. *Revista Jurídica Austral*, 5(1), 529-550. <https://doi.org/10.26422/RJA.2024.0501.con>
- Constitución Política del Perú. Art. 2. 29 de diciembre de 1993 (Perú).
- Corte Constitucional de Colombia. (2025). Sentencia T-067 de 2025 (Exp. T-8.202.533). 26 de febrero del 2025. <https://www.corteconstitucional.gov.co/relatoria/2025/T-067-25.htm>
- Corte Interamericana de Derechos Humanos. (2006). Caso Claude Reyes y otros vs. Chile. 19 de septiembre del 2006. https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf
- Decreto Legislativo 822 del 2025. Ley sobre el Derecho de Autor. Actualizada al 8 de julio del 2025. Diario Oficial El Peruano. <https://diariooficial.elperuano.pe/Normas/obtenerDocumento?idNorma=120026>
- Decreto Supremo 106-2017-PCM. Por medio del cual se aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN). 10 de noviembre del 2017. Diario Oficial El Peruano. <https://busquedas.elperuano.pe/dispositivo/NL/1585361-1>
- Delva Benavides, J. E., & Mendez Gonzalez, V. V. (2025). Algoritmos opacos y privacidad diferencial: ¿puede haber transparencia sin comprometer la protección? *FORSETI*, 14(22), 227-245. <https://doi.org/10.21678/forseti.v14i22.2834>
- Garrido, R., Lapostol, P., & Hermosilla, M. P. (2021). Transparencia algorítmica en el sector público. *Consejo para la Transparencia y GobLab Universidad Adolfo Ibáñez*. <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2021/10/>

ESTUDIO-TRANSPARENCIA-ALGORITMICA-EN-EL-SECTOR-PUBLICO-GOBLAB-cambio-tablas-1.pdf

- Juzgado Nacional en lo Civil 75. (2009). Pericia informática en el proceso Da Cunha, Virginia c. Yahoo de Argentina S.R.L. y Google Inc. 29 de julio del 2009. <https://www.csjn.gov.ar/archivo-cij/lib/pdfjs/web/viewer.html?file=%2Farchivo-cij%2Fadj%2Fpdfs%2FADJ-0.337882001248981920.pdf&v=2>
- Ley 1712 del 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. 6 de marzo del 2014. Diario Oficial No. 49.084. http://www.secretariassenado.gov.co/senado/basedoc/ley_1712_2014.html
- Ley 29733 del 2011. Ley de Protección de Datos Personales. 3 de julio del 2011. Diario Oficial El Peruano. <https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733>
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21. https://www.researchgate.net/publication/309322060_The_ethics_of_algorithms_Mapping_the_debate
- Morales Cáceres, A. M. (2021). El impacto de la inteligencia artificial en el derecho. *Advocatus*, (39), 39-71. <https://doi.org/10.26439/advocatus2021.n39.5117>
- Pauner Chulvi, C. (2023). Transparencia algorítmica en los medios de comunicación y las plataformas digitales. *Revista Española de la Transparencia*, (17), 107-136. <https://doi.org/10.51915/ret.308>
- Rivas Vallejo, P. (2021). Discriminación algorítmica: detección, prevención y tutela. XXXI *Jornades Catalanes de Dret Social (Treball, discriminación i COVID)*. https://www.researchgate.net/publication/354860623_Discriminacion_algoritmica_deteccion_prevencion_y_tutela
- Rousseau, J. J. (2017). *El contrato social*. Penguin. (Obra original publicada en 1762)
- Simon, J., Wong, P. H., & Rieder, G. (2022). El sesgo algorítmico y el enfoque del diseño sensible al valor. *Revista Latinoamericana de Economía y Sociedad Digital*, (1), 1-18. <https://revistalatam.digital/article/22tr02/?pdf=3400>
- Tribunal de Justicia de la Unión Europea. (2014). Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (Asunto C-131/12). 13 de mayo del 2014. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131>
- Weber, M. (2014). *Economía y sociedad: esbozo de sociología comprensiva*. Fondo de Cultura Económica. (Obra original publicada en 1922)