# informática y DERECHO

2ª Época

Revista Iberoamericana de Derecho Informático

Primer Semestre 2024 – Número 15 vol. 1

# informática y DERECHO

2ª Época

Revista Iberoamericana de Derecho Informático

(Primer Semestre 2024 – Número 15 vol. 1)

fiadi

Fundación
de Cultura
Universitaria

ISSN: 2530-4496

Editorial Fundación de Cultura Universitaria
25 de Mayo 583 - Tel. 2 916 11 52
CP 11.000 Montevideo - Uruguay
ediciones@fcu.edu.uy
www.fcu.edu.uy

# ÍNDICE

# ÍNDICE

# PRESENTACIÓN EDITORIAL

Queridas/os lectoras/es

En este 2024 se cumplen cuarenta años de la fundación de FIADI, que se produjo justo en 1984, cuando la informática y la tecnología comenzaban a adentrarse en la sociedad. No en vano, datan de esa década el internet más parecido a lo que se conoce hoy en día y la presentación de la primera computadora personal por parte de IBM, hechos que permitieron que la tecnología traspasara el sector gubernamental y de investigación y comenzarán a llegar a una mayor cantidad de personas de todos los ámbitos, incluido el académico.

En ese contexto, comenzaban a aparecer asociaciones defensoras de la informática jurídica, pero aunar a varias de esas asociaciones para constituir una Federación Iberoamericana de Asociaciones de Derecho e Informática suponía un logro sin parangón. En perspectiva, que esa Federación haya conseguido mantenerse, crecer y madurar, afrontando los retos del desarrollo y los cambios sociales, político-jurídicos y tecnológicos que han acontecido desde entonces, es sin duda un hito digno de mención y celebración.

Con motivo de este 40.º aniversario, hemos preparado, como regalo de cumpleaños, una edición especial de nuestra *Revista FIADI* en su segunda época. Por ello, este número 15 constará de dos volúmenes, que serán publicados de manera casi consecutiva en lo que resta del año, para los que se ha realizado una convocatoria pública de recepción de artículos que reflejen, desde cualquier perspectiva y de manera multidisciplinar, la relevancia del objeto de nuestra FIADI, esto es, la relación entre el binomio Derecho e Informática.

Ahora presentamos el primero de esos volúmenes que componen el número 15 de la Revista FIADI. En las páginas que a continuación se presentan, se da cabida a artículos de carácter eminentemente divulgativo que abordan una temática abierta vinculada al Derecho y la Informática.

El motivo por el que, en esta ocasión, no se han establecido ejes temáticos concretos que sirvan de base al número de la revista ha sido permitir a todos quienes quisieran participar con sus artículos en este volumen de la Revista, a modo de regalo del cumpleaños de FIADI que celebramos, poder hacerlo, sea cual fuera el área de trabajo en la que se encontraran más cómodos. El único límite que se estableció fue que guardaran relación, directa o indirecta, con el fin de la Federación, esto es, según sus estatutos, la cooperación, la promoción, el estudio, el intercambio de experiencias y la gestión y desarrollo de soluciones en torno a la informática jurídica, la informática forense y el derecho informático

o el derecho aplicable a las tecnologías de la información y la comunicación en general.

Cumpliendo este requisito se han seleccionado15 artículos, tras un análisis llevado a cabo por revisores expertos en la materia, a los que, desde aquí, no podemos dejar de agradecer su labor. El número en sí no es arbitrario, sino que se ha querido hacer coincidir con el número de la Revista, en su segunda época, que se presenta por una cuestión de simbología en este cumpleaños.

Del total de artículos, 14 abordan en perspectiva nacional, europea o internacional temas de actualidad y relevancia jurídica que, en tono académico, e informativo, abordan distintos aspectos de la materia objeto de estudio. Entre los temas analizados se encuentran los siguientes:

Por un lado, algunos temas de carácter normativo, como son los que versan sobre el Reglamento Europeo de *e-evidence* y su relación con la protección de datos, el estatuto jurídico de los proveedores de servicios de intermediación en línea a la luz del Reglamento Europeo de plataformas digitales o la protección de los derechos de autor frente a las creaciones realizadas con inteligencia artificial.

Por otro lado, temas vinculados a cuestiones transversales políticas, jurídicas y sociales, como los que estudian los desafíos de la gobernanza en internet en esta era de convergencia tecnológica, los efectos colaterales de la brecha digital en relación con la ciberseguridad y el peligro de la irrelevancia si no se afronta la transformación digital.

Se afrontan también los problemas éticos y la afectación a los derechos humanos derivados del uso de la inteligencia artificial y algunas obligaciones, vinculadas a la transparencia, que se han diseñado para tratar de minimizarlos.

Por último, se presentan análisis específicos y sectoriales de otros temas relevantes, como son las implicaciones del *blockchain* y la seguridad de la información en América y Europa, el debate sobre si los criptoactivos son o no dinero y su afectación en relación con el Proyecto Ágora mexicano, los retos en cuestión de protección de datos que plantea la Estrategia Nacional de República Dominicana sobre Inteligencia Artificial y el coste de acceso a la justicia administrativa del Tribunal Supremo en Venezuela y su relación con el uso de las TIC.

El artículo restante se presenta como preámbulo, a modo de semblanza, dado el sentir de alguien que vivió, en primera persona, el nacimiento de la Federación Iberoamericana de Asociaciones de Derecho e Informática, que ahora llega, sin atisbo de crisis, a la cuarentena. Por ello, este artículo, de menos rigor científico, cumple la finalidad de recordar a todos, a los más jóvenes y a los más antiguos, cuál fue el contexto en el que vio la luz la FIADI, lo que supuso y lo que se ha avanzado desde entonces.

A nivel personal, no puedo más que dejar constancia de que «bautizarme» como editora de la *Revista FIADI* en su segunda época en este preciso momento resulta un verdadero placer, motivo por el que quiero aprovechar para dar las gracias a la Directiva de FIADI, por la confianza depositada en mí para llevar a cabo esta tarea, a la par que una gran responsabilidad que espero saber asumir, con respeto y ánimo.

A la FIADI, teniendo en cuenta que comparto la idea de quienes consideran que «los cuarenta son los nuevos veinte», ¡solo puedo desearle una larga vida y un muy feliz cumpleaños!

Finalmente, solo resta agradecer a quienes han colaborado en este primer volumen con sus aportes y su evaluación, a quien me ha precedido en esta fantástica labor como editora, la Dra. Yasna Bastidas Cid, y al director académico de la Revista, Dr. Heriberto García Peña, por su confianza, apoyo incondicional y gran comprensión en mi estreno; y a ustedes, queridos/as lectores/as, por seguir acompañándonos en una nueva edición de la *Revista Informática & Derecho* en su segunda época.

¡Nos veremos de nuevo en el volumen 2!

Atenta y cordialmente,

Prof.ª Dra. Lucana Estévez Mendoza

Editora general

Junio de 2024

# PREFACIO

Fue hace cuarenta años, el 30 de octubre de 1984, cuando un grupo de especialistas en derecho y en informática de diversos países de Iberoamérica fundaron en Santo Domingo, República Dominicana, la *Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI),* como un foro dedicado al estudio de los diferentes temas vinculados entre el derecho y la informática.

Para entonces se había hecho necesaria la existencia de una entidad académica dedicada al estudio e investigación de estos temas relacionados con una nueva rama del derecho, como era en ese momento el derecho informático.

Así surgió FIADI, como una organización internacional para nuclear tanto a asociaciones de derecho e informática, como a miembros individuales.

La misión de la FIADI desde su comienzo ha sido fomentar el estudio, promoción y desarrollo del derecho de la informática y las tecnologías de la información y la comunicación (TIC) en la región iberoamericana, impulsando la cooperación, el intercambio de conocimientos y experiencias entre sus miembros, así como creando colaboraciones con entidades académicas, gubernamentales y del sector privado.

Su destino pretendía ser convertirse en una referencia en el ámbito del derecho y las TIC que contribuyera al avance de la legislación, las políticas públicas y la formación de profesionales preparados para enfrentar los desafíos legales y las oportunidades que plantean las tecnologías de la información en nuestra sociedad.

Fue allí, en Santo Domingo en este Congreso de 1984, donde se eligió al primer presidente de FIADI, Miguel López Muñiz Goñi, quien tuvo destacada actuación en ese Congreso y en los siguientes años.

Como bien dice Antonio Martino en su artículo *Hace 40 años. Rememorando*, publicado en este número de la revista:

> El congreso tuvo dos méritos innegables: el haber reunido por primera vez en Latinoamérica tantos especialistas en informática jurídica y el haberse decidido formar la Primera Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI) como entidad dedicada a la promoción, estudio y desarrollo de la informática jurídica, la informática forense y el derecho informático y de las nuevas tecnologías en general.

El afianzamiento de FIADI se ha ido produciendo durante un largo proceso en estos cuarenta años, conducido por especialistas de Iberoamérica, destacando

entre ellos fundamentalmente la figura de Valentín Carrascosa López, quien fuera un visionario en el ámbito del derecho informático y quien ejerciera durante varios períodos la presidencia de la Federación.

En cuanto a la fase institucional, en 2015, por iniciativa de Julio Téllez Valdés, se aprobaron en Medellín, Colombia, los estatutos que se protocolizaron y aprobaron luego de manera definitiva en Montevideo, Uruguay, en diciembre de ese mismo año, obteniendo así su plena personalidad jurídica.

Desde su inicio, periódicamente se han celebrado Congresos en diversos países, todos con un gran nivel académico, entre los que cabe mencionar los Congresos de Santo Domingo, República Dominicana (1984); Guatemala (1989); Mérida, España (1992); Bariloche, Argentina (1994); La Habana, Cuba (1996); Montevideo, Uruguay (1998); Lima, Perú (2000); México, D. F. (2000); San José, Costa Rica (2002); Santiago de Chile (2004); Panamá (2006); Zaragoza, España (2008); Lima, Perú (2009); Universidad Autónoma de Nuevo León, Monterrey, México (2010); Universidad Católica, Buenos Aires, Argentina (2011); Universidad de las Américas, Quito, Ecuador (2012); Santa Cruz, Bolivia (2013); San José, Costa Rica (2014); Universidad Pontificia Bolivariana, Medellín, Colombia (2015); Universidad de Salamanca, Salamanca, España (2016); Universidad Autónoma de San Luis Potosí, San Luis Potosí, México (2017); Universidad Tecnológica de Panamá, Ciudad de Panamá, Panamá (2018); Asociación de Abogados de San Pablo, San Pablo, Brasil (2019); Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León, Monterrey, México (2022); Universidad de Villavicencio, Villavicencio, Colombia (2023).

En estos cuarenta años de FIADI, a través de ella he conocido a grandes especialistas del derecho informático, con los que en muchos casos he creado una amistad. Recuerdo especialmente a Valentín Carrascosa, quien me honra con su amistad; a Julio Téllez Valdés, quien con sus libros, *papers* y conferencias mucho me ha enseñado.

Me vienen a la memoria otros nombres: Juan Diego Castro, Pedro Patrón, Marcelo Bauzá, Mirna García Barrera, Yarina Amoroso, Augusto Ho, Federico Bueno de Mata, Mariliana Rico, Heriberto García Peña, Bibiana Luz Clara, Rodrigo Cortés Borrero, Humberto Ruani, Karina Céspedes, Patricia Reyes, Ernesto Ibarra, Lorenzo Cotino, Antonio Martino, Luis Fernando Martins Castro, Jaqueline Guerrero, Carlos Reusser, Carmen Velarde, y tantos otros que por cuestión de espacio no menciono.

De manera especial quiero recordar a Álvaro Andrade Sejas, quien nos dejó hace algunos años y quien me regaló momentos inolvidables en una visita a Ávila y Segovia.

El próximo XXVI Congreso se realizará este año, coincidiendo con el lugar de su fundación, en Santo Domingo, República Dominicana, en la Pontificia Universidad Católica Madre y Maestra, oportunidad en que, como en otras ocasiones, se proclamará un nuevo premio Valentín Carrascosa, en su octava edición.

Los nueve ejes temáticos de este Congreso reflejan la actualidad y avances del derecho y la informática en los últimos años: inteligencia artificial; ciberseguridad, prevención e investigación del ciberdelito; justicia digital, proceso

electrónico y resolución de conflictos en línea; telecomunicaciones y transporte autónomo; derechos digitales y neuroderechos; economía digital y contratación electrónica; manipulación de la naturaleza: genómica, climática; protección de datos personales y privacidad e innovación tecnológica del derecho (*Legaltech*).

He participado en muchos de los Congresos FIADI y si bien no puedo destacar a ninguno en particular, si puedo afirmar que todos han reunido un alto nivel académico y sus temáticas se han ido adecuando a los nuevos temas clave del Derecho Informático de cada momento.

FIADI también ha creado una revista, la Revista Iberoamericana de Derecho Informático, que cumple ahora quince años, en su segunda época y de la cual tengo el honor de prologar este primer tomo. Este tomo consta de quince artículos de carácter eminentemente divulgativo, que abordan cuestiones de derecho e informática y que espero disfruten con su lectura.

Horacio Fernández Delpech

# PREÁMBULO

# HACE 40 AÑOS. REMEMORANDO

*40 YEARS AGO. REMEMBERING*

**Antonio A. Martino**

Profesor de la Universidad de Pisa (Italia) y la
Universidad del Salvador (Argentina)
Miembro de número de FIADI

*La idea de los derechos no es otra cosa que la idea de la virtud introducida en el mundo político. Es con la idea de los derechos con la que los hombres han definido lo que eran la licenciosidad y la tiranía (…). No hay grandes hombres sin virtud; sin respeto a los derechos no hay gran pueblo: casi se puede decir que no hay sociedad; porque ¿qué es una reunión de seres racionales e inteligentes en la que la fuerza es la única relación?*

Giuseppe Chiovenda (1872-1937)

*El mercado para los ordenadores personales está muerto. La innovación ha cesado, virtualmente. Microsoft domina con muy poca innovación. Se acabó. Apple perdió. Ese mercado ha entrado en la Edad Oscura, y va a estar en esa Edad Oscura durant*e los próximos diez años.

Steve Jobs (2006)

*El derecho se transforma constantemente. Si no sigues sus pasos, serás cada día un poco menos abogado.*

Herbert L. A. Hart (1907-1992)

## El contexto: la circunstancia

Al principio eran las líneas naturales que dibujaban en el paisaje las vías por las cuales cosas y personas se movían de un lugar al otro. El perfil de un río, las aguas tranquilas de un mar interior, pero luego apareció la obra del hombre, transformando el paisaje y creando verdaderas vías de comunicación: los caminos.

Para señalar lo que eran los límites del mundo de aquel momento fueron creadas las vías romanas, que perduran en el tiempo. A veces esas vías no son más que una organización, tal que una caravana va dibujando en el paisaje la posibilidad del desplazamiento y esto hace que una civilización florezca. Luego llegó la época de las grandes vías navegables y al pasar más allá del océano la redondez del mundo tuvo su factibilidad.

A partir de entonces, latitudes y longitudes significaron la posibilidad de desplazamiento y de situación: recolocamiento. Pero es el vuelo aéreo el que da la posibilidad de un mundo mucho más cercano en el cual, a partir de cualquier lugar, se puede estar en el centro de todo el mundo.

Finalmente, a través de los medios de comunicación modernos, de los teléfonos, de la radio, del télex, del telefax y de las redes de computadoras, los celulares y WhatsApp, el globo se vuelve instantáneo. La diferencia de latitudes y longitudes se anula en el tiempo de la comunicación, y las vías del desarrollo se reducen prácticamente a una sola: estar dentro de la red que vincula cada lugar del mundo con todos los otros.

A principios de los ochenta no existía internet, pero había mucho trabajo de informática jurídica. La doctrina la había dividido en documental, de gestión y de ayuda a la decisión[1].

El 30 de abril de 1980, el Consejo de Europa, al adoptar la Recomendación «Informática y Derecho», fomentó la enseñanza, la investigación y la difusión en el ámbito de la informática y el derecho. La Recomendación preveía, en particular, considerar el ordenador como una herramienta fundamental para uso del jurista, así como investigar sistemáticamente, además de los problemas específicos de la informática, también las aplicaciones y los instrumentos jurídicos relacionados con la protección de los datos introducidos en los ordenadores y la seguridad informática.

Sin embargo, el objetivo de la rápida circulación de la información mediante el uso de la informática exigía la digitalización previa de los datos (es decir, que toda la información se escribiera en código binario para que los ordenadores pudieran indexarla), sentando así las bases para la difusión del tratamiento de textos o una nueva forma de escribir: con un nuevo alfabeto, el alfabeto binario; con una nueva tinta, la de los electrones; sobre un nuevo soporte, las memorias electrónicas.

1 Debo reconocer que en mis primeros escritos la llamé «informática jurídica de decisión». Los franceses del IRETIG me hicieron notar que era mejor «ayuda a la decisión».

En este contexto, en 1983 había asumido la dirección del Instituto de Documentación Jurídica del Consejo Nacional de Investigaciones italiano (hoy Istituto d'Informatica Giuridica e Sistemi Giudiziari) con sede en Florencia y nos ocupábamos entonces de la informática jurídica[2], y empezábamos a otear las aplicaciones de la informática al razonamiento jurídico. De ahí el título del número monográfico *Logica, informática, diritto,* que preanunció los cuatro congresos con ese nombre que hicimos en Florencia en 1981, 1985, 1989 y 1993, es decir, cada cuatro años, mientras que las actas fueron publicadas por Elsevier[3].

En ese primer fascículo colaboraron los curadores: Ciampi, Maretti y Martino, Jercy Wrobleski, Alexander Peczenick, Jon Bing, Carlos E. Alchourron, Giuliano Di Bernardo, Miguel Sanchez Maza y Amedeo Conte, todos bajo el manto tutelar de Georg H. von Wright.

Por otro lado, Mario Losano y Vittorio Frosini habían propugnado el nombre de «informática jurídica» en vez de «jurimetría», como se le conocía también[4].

Algunos autores distinguían entre derecho informático como el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática, mientras que la informática jurídica era considerada el resultado del impacto de la tecnología en la ciencia del derecho.

En Estados Unidos, un profesor de Michigan, Leyman Allen, había publicado ya libros que causaron no poco revuelo[5], por la introducción de términos lógicos y matemáticos en el derecho. Los estudios de abogados comenzaban a utilizar la informática y la American Bar Association financió la creación de cuarenta cátedras de informática jurídica en todo el país.

Las empresas, sobre todo las grandes, usaban métodos de recopilación de datos y de transferencia de los mismos a sus sucursales, estuviesen en el país o en el exterior. A eso se le llamaba *Electronic Data Interchange* (EDI).

Para resolver los problemas de estandardización, la entonces Comunidad Económica Europea, los Estados Unidos y casi todos los países que comenzaban a utilizar estos medios crearon una institución llamada Edifact que, a través de

2 *Rivista Informatica e Diritto, Fascicolo II*, 1978, Le Monnier, Firenze, Ciampi, Maretti, Martino, número monográfico, *Logica, informatica, diritto*.

3 Martino, A. (Ed.), *Deontic Logic, Computational Linguistics and Legal Information Systems*, Vol. II, Ámsterdam, Nueva York, Oxford, North-Holland, 1982; Martino, A., Socci Natali, F. (Eds.), «Automated Analysis of Legal Texts», *Logic Informatics, Law*. Ámsterdam, North-Holland, 1986 y Martino, A. (Ed.), *Expert System in Law*, Ámsterdam, Nueva York, Oxford, Tokio, North Holland, 1992.

4 Losano, M. G., *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Turín, 1969; Frosini, V., *Cibernetica, diritto e società*, Milán, 1968.

5 Allen, L., *Ecuaciones: el juego de las matemáticas creativas*. Ed. Rev. New Haven, Connecticut: Publicación de materiales educativos de Autotelic, 1969. *El juego de los números reales*. New Haven, Connecticut: Publicación de materiales educativos de Autotelic, 1966. «Hacia un lenguaje normalizado para aclarar la estructura del discurso jurídico», en Lógica Deóntica, Lingüística Computacional y Sistemas de Información Jurídica, editado por Martino A, 349-407. vol. 2, y luego en versiones editadas de artículos seleccionados de la Conferencia Internacional sobre «Lógica, Informática y Derecho», Florencia, Italia, 1981. Ámsterdam: North-Holland Publishing Company, 1982.

diferentes comisiones, afrontaba la estandardización de todos los documentos que pertenecen a cada una de las ramas de los sectores económicos.

Se había creado la Asociación Europea de EDI, formada por los representantes de los países que formaban la Comunidad Económica Europea (antecedente de la Unión Europea). Una de las comisiones que se creó dentro de la Comunidad fue la de determinación de la forma de los documentos electrónicos. A la sazón yo era el presidente de la Asociación de Ediforum Italia[6], así que tuve que ir y participar en las reuniones.

Comenzamos por la factura, que no tenía ninguna forma especial en el papel, pero a la cual hubo que darle una forma en informática, y seguimos por cada uno de los documentos comerciales. Llegamos a tipificar más de 270 documentos.

Cada país representaba los intereses de sus empresas y todos querían imponer los criterios que ya estaban usando, por lo tanto, las semanas anteriores a la reunión pedía instrucciones a las empresas italianas que me daban puntos para defender, sabiendo que tenía que negociar, pues los otros países también tenían criterios nacionales para defender.

Fueron reuniones épicas, casi todos eran informáticos y yo el único jurista. En 1986 se incorporaron España y Portugal, y recuerdo una anécdota risueña: nos reuníamos los segundos martes de cada mes en Bruselas a las 10, pero los representantes de estos dos países recién incorporados llegaban a las 12.30 o 13. Un día el español me invitó a almorzar y me preguntó si nos molestábamos porque ellos llegaban algo tarde, le contesté que no y que si venían directamente a las 14 podíamos ir a almorzar derechamente, pues antes que ellos llegaran nosotros votábamos. Se iluminó su cara con un destello de rabia y vergüenza. A partir de entonces fueron los primeros en llegar.

En Francia, el Instituto de Investigación en Tecnologías de la Información y la Comunicación (IRETIG) era centro de investigación del Consejo Nacional de Investigaciones del país (CNRS), centrado en la informática jurídica, con sus sedes en París y Montpellier, bajo la dirección de Pierre Catala, uno de los pioneros de la informática jurídica[7] y creador de una base de datos jurídica, Juris-Data.

En Italia estábamos nosotros, el IDG, en Florencia y en Roma la casación italiana con su sistema Italgiure y la base de datos de la legislación en la Cámara de Diputados.

6 No por méritos, sino porque la asociación estaba formada por grandes empresas como Fiat, Montedison, Pierelli, Eni, Luxottica, Enel, Ferrero, Intesa Sanpaolo, etc. que desconfiaban entre sí, pues había grandes intereses en juego, mientras que yo representaba a un ente estatal dedicado al estudio como el Consejo Nacional de Investigaciones y, por lo tanto, no era un competidor.

7 Bing J., «Let there be LITE : a brief history of legal information retrieval [archive]», *in European Journal of Law and Technology*, Vol. 1, Issue 1, 2010. Años después invite a Pierre a Florencia donde pronunció unas conferencias inolvidables que quise publicar con el nombre de *Pierre Catala en Florencia,* pero cada vez que mandaba el definitivo volvía a corregirlo y luego de su muerte me ha quedado la última versión en borrador.

En Latinoamérica había asociaciones de estudio y difusión de la informática jurídica y algunos centros de datos jurídicos como el Saij argentino y el Prodasen brasileño.

La Oficina Intergubernamental para la Informática, cuyo nombre original es *Intergovernmental Bureau for Informatics* (IBI), surge como una transformación del Centro Internacional de Cálculo (ICC: *International Computation* Centre) que fue creado por la Unesco en 1951, por Resolución 2.24 de su Conferencia General, después de muchos avatares que no es el caso tratar aquí, con sede en Roma a fines de los años setenta.

> A inicios de la década de 1970 una pequeña organización internacional, constituida en sus inicios de la mano de la UNESCO, iniciaba una trayectoria tan impactante como fugaz. El IBI (Oficina Intergubernamental de Informática), con sede en Roma, liderado por el argentino Fermín Bernasconi, desarrolló una intensa actividad destinada a producir la toma de conciencia de las élites del Tercer Mundo (3M) acerca de «la revolución de la Informática». (…) su sostén financiero dependía en gran parte de los aportes de tres estados europeos: Francia, Italia y España. El IBI tuvo una particular presencia en América Latina, donde contó con 13 países miembros y promovió iniciativas relevantes para la autonomía y la integración regional[8].

El IBI se preocupó mucho por el fomento y desarrollo de la formación en Informática. A tal efecto creó un Centro Regional para la Enseñanza de la Informática (CREI), en 1976 con sede en Madrid (España), en colaboración con el gobierno español.

El CREI hacía la convocatoria de Santo Domingo, que fue muy apreciada y seguida por los estudiosos y funcionarios de la época. Decidí participar haciéndolo coincidir con un viaje a Brasil donde visité el Prodasen (Banco de Datos del Senado Federal). Venía de una larga colaboración con entidades brasileñas y decidí aceptar la invitación del Prodasen, en Brasilia[9], y de la Universidad de San Pablo, que estaba comenzando programas de informática jurídica en la cátedra de Filosofía del Derecho de Miguel Reale, donde comenzaba a destacarse Tercio Sampajo Ferraz.

Las comunicaciones con Santo Domingo no eran fáciles, así que tuve que tomar un avión a Caracas y allí me informaron que no había avión directo a Santo Domingo, sino que había que hacer escala en Willemstad, capital de Curazao. Así lo hice y en el avión que iba a Willemstad me encontré con un viejo amigo argentino, el profesor Ricardo Guibourg, quien también iba al Congreso[10].

8 Cito directamente del trabajo de Carnota, R., *Informática y Soberanía. El IBI y la integración latinoamericana y caribeña,* 2018. https://www.researchgate.net/publication/359207284_Informatica_y_Soberania_El_IBI_y_la_integracion_latinoamericana_y_caribena. Las luchas de poder hicieron retirarse a Francia y España y finalmente Italia decidió no colaborar más.

9 El Prodasen (Programa de Modernização e Integração dos Poderes Judiciário e do Ministério Público do Brasil) es un programa de modernización e integración de los poderes judiciales y ministeriales en Brasil.

10 Corroboré con el Prof. Guibourg y tiene los mismos recuerdos, por lo cual deducimos que debe ser verdad todo lo que recordamos.

La llegada a Santo Domingo fue espectacular, por el clima tropical, por la historia y por lo que esperábamos vivir. Si bien Rafael Leónidas Trujillo Molina, dictador sanguinario, había sido asesinado en 1961, todavía podían visitarse los lugares de su dictadura y donde se vivió toda esa historia muy latinoamericana[11]. Nos recibieron con mucha atención y nos pusieron un guía turístico, que no era muy competente, pero sí gracioso y atento.

La ciudad con un centro histórico amurallado y adoquines, la zona colonial, tiene edificios que datan del siglo XVI, incluida la catedral, que fue la primera construida en el Nuevo Mundo. En la Plaza de España, bordeada de cafés, se encuentra el palacio Alcázar de Colón, así que hubo mucho para ver.

El congreso tuvo dos méritos innegables: el haber reunido por primera vez en Latinoamérica tantos especialistas en informática jurídica y el haberse decidido formar la Primera Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI) como entidad dedicada a la promoción, estudio y desarrollo de la informática jurídica, la informática forense y el derecho informático y de las nuevas tecnologías en general.

Poco tiempo después fue creado también el Instituto Latinoamericano de Alta Tecnología, Informática y Derecho (ILATID), con sede en Buenos Aires, pero al cabo de una década dejó de funcionar.

## El congreso

Fue un congreso magnifico por su composición, por la participación, por lo que se hizo en él y por los resultados que tuvo[12].

El comité de honor estuvo constituido por el presidente de la República Dominicana, Salvador Jorge Blanco, el ministro de Cultura de España, Javier Solana, el presidente del CREI, Guillermo de Ávila y Dueña, el embajador de España en Santo Domingo, José Luis Pérez Ruiz y el presidente del IBI, Fermín Bernasconi.

El comité organizador fue un lujo en Iberoamérica: Miguel López Muñiz, su presidente, en nombre de Aside, la Asociación de Informática y Derecho de España y Emanuel Esquea Guerrero, consultor jurídico del Poder Ejecutivo dominicano.

Entre los vocales se encontraban Ildefonso Guillermo Clavijo, por la Asociación Argentina de Informática Jurídica; Antonio Pojo Do Rego, por la Asociación Brasileña de Informática Jurídica; Alfonso Reyes Echandía, por Colombia; Jorge Raúl Cabañas, por Paraguay; Luis Rosario Vilches, por Perú; José Nilo Dávila, por Puerto Rico y Nicolás Vega, por Venezuela.

11 Magistralmente reflejada en la novela de Vargas Llosa, *La fiesta del Chivo*, Alfaguara, 2006.

12 Todos los datos del congreso los he corroborado con las actas del mismo que me facilitara Marcelo Bauzá, alma y continuador del FIADI y me han servido para comparar, completar y regenerar los recuerdos que ya mi vieja mente aun contiene.

El secretario era el gran factótum del encuentro, Benito Roldan Casañé, director del CREI.

El congreso eligió como presidente a Carlos Suárez Anchorena, subsecretario de Asuntos Legislativos de Argentina, como vicepresidente a Enrique Pochet, viceministro de Justicia de Costa Rica, y como presidentes de sesiones a Miguel López Muñiz Goñi, presidente de Asise en España, Federico Carlos Álvarez, presidente de la Asociación Dominicana de Informática Jurídica, Daniel León García, presidente de la Academia de Informática Jurídica de México y Jaime Giraldo Angel, profesor de la Facultad de Derecho de los Andes, Colombia[13].

Este enjundioso congreso se celebró desde el 29 de octubre al 2 de noviembre, con una actividad ejemplar, dirigida por el infatigable Benito Roldán Caseñé[14]. Vivimos «disfrutando la excelencia de las exposiciones, la vehemencia de los debates y el valor de las conclusiones»[15].

La presentación se hizo en el auditorio del Banco Central de Santo Domingo. El día 29 hablaron Benito Roldán, Manuel Bergen Chupani, presidente de la Corte Suprema de Santo Domingo, López Muñiz y el presidente de República Dominicana, Salvador Jorge Blanco.

A continuación, se hizo una exposición de los presidentes de las asociaciones nacionales, quienes describieron el estado del arte en ese momento en cada país: Argentina, Brasil, Colombia, Costa Rica, Chile, España, Guatemala, Puerto Rico y Venezuela.

El punto de mayor interés consistió en el proyecto de creación de la Federación Iberoamericana de Asociaciones de Derecho e Informática, que agrupa a las asociaciones nacionales con una directiva, un consejo rector, la presidencia, dos vicepresidencias y una secretaría permanente.

El martes 30 de octubre por la mañana, a las 12, en una sesión presidida por Miguel López Muñiz Goñi, se creó la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI), se aprobaron los estatutos y se eligió la Junta Rectora. Por la tarde, sesionó la Comisión de Informática Jurídica Documental, coordinada por Federico Carlos Álvarez, de República Dominicana, donde expusieron Carlos Suárez Anchorena, de Argentina, Patricio Navarro, de Chile y José Nilo Dávila, de Puerto Rico.

13 Giraldo de algún modo siguió luego la obra de Reyes Echandía en la Corte Suprema colombiana favoreciendo el uso y el estudio de la informática jurídica. En 1990 el presidente César Gaviria lo nombró como Ministro de Justicia hasta el 1991, desde su ministerio impulsó la política de sometimiento a la Justicia mecanismos para combatir y contrarrestar la arremetida del narcoterrorismo, logró la entrega de importantes narcotraficantes como: Hermanos Ochoa, Pablo Escobar, Roberto Escobar Gaviria y Jhon Jairo Velásquez Vásquez.

14 Benito Roldán era ingeniero, acostumbrado a las ciencias duras que estaba algo asombrado de la ductilidad y digámoslo también, ambigüedad del derecho, pero que supo acomodarse y dirigirnos con la pulcritud del ingeniero y con una delicadeza de embajador. Al final hizo mucho más que este congreso por Latinoamérica, pero no es para tratarlo aquí.

15 Cito del prólogo de Benito Roldán a la presentación del Congreso.

El día 31 sesionó la Comisión de la Enseñanza de la Informática para profesionales del derecho, coordinada por Daniel León García, de México, y donde expusieron Abelardo Rivera Llanos, de Colombia, Eduardo Hajna Rifo, de Chile y Fernando Galindo Ayuda, de España. Por la tarde se reunió la Comisión del Derecho en la nueva Sociedad Informativa, coordinada por Jaime Giraldo Angel, colombiano, y donde expusieron Ricardo Guibourg, de Argentina, Luis Carlos Bettiol, de Brasil, Edgar Salazar Cano, de Perú y Carlos Ruiz González, de México.

El 1 de noviembre por la mañana sesionó la Comisión de Lenguaje, Lógica y Derecho, coordinada por Alfonso L. García Martínez, de Puerto Rico, donde expusieron Antonio Anselmo Martino, de Argentina, Jaime Giraldo Angel, de Colombia, Miguel López Muñiz Goñi, de España y también el español Miguel Sánchez Mazas[16]. Por la tarde sesionó la Comisión de Informática en la Gestión de Justicia, coordinada por Rodolfo Bolaños Ramírez, de Guatemala, con las exposiciones de Antonio Millé, de Argentina, Ignacio Carillo Prieto, de México, Francisco Moreno y Carlos Losada de España.

El 2 de noviembre, el congreso culminó con la proclamación de los estatutos de FIADI por Miguel López Muñiz Goñi, presidente electo, y la lectura de las conclusiones por parte de Enrique Pochet Cabezas, vicepresidente del congreso. Se les entregó un memorial CREI a las autoridades por parte de Benito Roldan, director del CREI y los discursos de Carlos Suárez Anchorena, presidente del congreso y José Luis Pérez Ruiz, embajador de España. El discurso de clausura estuvo a cargo de Américo Espinal, procurador general de República Dominicana.

El congreso tuvo momentos tocantes, como el del discurso del primer mandatario de la República Dominicana, recordando los quinientos años de la llegada de los españoles «a estas tierras y Santo Domingo fue el foco irradiador de la Fe, la Cultura y el Derecho (…) ha llegado el momento de intercambiar ideas. No podemos seguir avanzando por caminos paralelos (…) aprovechemos nuestra identidad en la estructura jurídica y en la lengua»[17] y también las demostraciones de los sistemas iberoamericanos de informática jurídica que se hicieron en el congreso.

Sin dudas el hecho saliente fue la creación de FIADI, su mesa directiva, un consejo rector, la presidencia y dos vicepresidencias y una secretaría permanente. Las personalidades que han regido los destinos de FIADI en estos cuarenta años nos iluminan sobre el coraje, la determinación y el enorme trabajo que permitieron a la institución de sobrevivir y ser rectora y aparecen sobresaliendo en todos estos años, mientras otras entidades sucumbían o desaparecían. El paso del tiempo se llevó consigo muchas de esas extraordinarias personas, pero no pudo destruir el proyecto y su realización.

16 Con Miguel trabamos una sólida amistad, cimentada en los congresos Lógica, informática, derecho, mencionados antes y las invitaciones a San Sebastián, donde expusimos por primera vez *Lógica sin verdad*, con Carlos Alchourron y fue publicada en la *Revista Theoria*, que dirigía Sanchez Mazas, vol. 3, n.º 1/2/3, octubre-septiembre 1987-1988.

17 Cito del discurso de Jorge Blanco, presidente de República Dominicana.

En las conclusiones se notó la solidaridad iberoamericana y la coincidencia en la necesidad de proclamar y fomentar la transferencia recíproca de logros, beneficios y adelantos en este campo basada en el principio de integración regional como instrumento indispensable para el arraigo, desarrollo y crecimiento de la cultura informática.

De las ponencias que fueron presentadas no es el caso de escribir en este artículo, pero no puedo olvidar de hacer una referencia a la que presenté en la mañana del 1 de noviembre: *Contaminación legislativa y remedios informáticos*[18], porque dio lugar a la creación de una maestría en la Universidad de Pisa, Italia, sobre ciencia de la legislación, en 1986 y luego otra en la Universidad del Salvador, Argentina, con el mismo nombre, en 1992. De ellas surgió la idea de hacer una revisión de todas las leyes promulgadas para averiguar cuáles estaban en vigor. En Italia, la idea tomó cuerpo hasta que algunos políticos la transformaron en un caballito de batalla[19] y fracasó científicamente.

En Argentina tuvo mejor suerte, pues dio lugar a que el 20 mayo de 1988 el Congreso argentino sancionara la Ley del Digesto que autoriza la reordenación de todas las leyes. El 18 de junio el Poder Ejecutivo la promulgó con el n.º 24.967.

Para realizar el Digesto Jurídico Argentino, así como lo quería la Ley, el Ministerio de Justicia llamó a una licitación pública, en la cual se presentaron diferentes grupos. Un consorcio entre la Facultad de Derecho de la Universidad de Buenos Aires y las principales empresas de publicación de textos jurídicos (La Ley, Jurisprudencia Argentina y El Derecho) ganó la licitación, y allí empezó la aventura.

En agosto de 1999 comenzó la empresa dividida en dos partes: una, relativa a la redacción de un Manual de Técnica Legislativa, y otra, mucho más grande, encargada de revisar todos los textos normativos emanados a partir de la Constitución de 1853.

La primera parte, coordinada por quien escribe, contó con un grupo de juristas lingüistas italianos, juristas documentalistas argentinos, juristas informáticos italianos y miembros del Istituto per la Documentazione Giuridica del Consejo Nacional de Investigaciones italiano, que dirigí entre 1983 y 1992.

La revisión de todas las leyes y decretos reglamentarios ha sido una obra muy fatigosa y realmente monumental, realizada por un personal especializado de juristas, lingüistas, informáticos y documentalistas que ha rondado la centena, dirigidos todos por el profesor Atilio Alterini (director general) y compuesta por los Dres. Ramón Brenna (director técnico), Daniel Altmark (coordinador ejecutivo) y Horacio Álvarez (director académico). Para que pudiera funcionar este

18 Martino, A. «Contaminación legislativa y remedios informáticos», Ágora: la informática en un mundo en transformación, n.º. 1985/2 11 (ejemplar dedicado a las tendencias informáticas), pp. 21-22.

19 Maurizio Balocchi, ministro del gobierno Berlusconi de *Semplificazione normativa*, hasta el 14/2/2010, luego Francesco Belsito y finalmente Roberto Calderoli, quien protagonizó una quema de libros que probablemente contenían leyes en una actuación por televisión. Calderoli fue autor de la ley de voto político italiana que él mismo considero «una chanchada». Hoy es ministro del gobierno de Meloni.

enorme engranaje, fue creada *ad hoc* una parte nueva del edificio de la Facultad de Derecho de la Universidad de Buenos Aires gracias a la audacia y al tesón de su entonces decano, Andrés D'Alessio.

El Manual finalizó en el 2001, el resto tardó más tiempo, pero fue terminado y entregado a la Comisión bicameral, que lo aprobó, y en 2014 se promulgó la Ley 26.939 del Digesto Jurídico Argentino. Se revisó 32.000 leyes, se determinó que estaban en vigor solo 3.144 y las restantes 29.000 fueron derogadas[20].

Por razones que los juristas sabrán explicar, no obstante, todo el Digesto Jurídico Argentino no se aplica por parte de jueces y abogados[21], por eso he realizado una publicación solicitada por Mario Bunge sobre el tema[22].

## Conclusiones

En estos cuarenta años, la labor de FIADI ha sido infatigable. Ha continuado con el espíritu de Santo Domingo, sin importar quién haya estado en su faz directiva.

No me toca a mí hacer un balance, pues ello requeriría una capacidad historiográfica y la disponibilidad de datos completos, de los que carezco. Ha habido ya una primera historia contada por Valentín Carrascosa y María Teresa Molina, con el título *Fiadi y su aportación al área de la informática y el derecho,* a la que me remito[23]. Pero, habiendo osado a hablar del congreso de Santo Domingo, me arriesgo a escribir algo, a modo de conclusión.

El espíritu de Santo Domingo ha perdurado en estos cuarenta años en modos tangibles: por los congresos internacionales que han continuado celebrándose[24], tiene un sitio en internet[25] y participa en la mayor parte de las redes sociales conocidas: Instagram, Facebook[26], X, LinkedIn, etc. Tiene una revista sobre infor-

20 En el Saij, Sistema argentino de informática jurídica, se encuentran los dos archivos con las leyes aprobadas y las derogadas. www.saij.gob.ar/24967-nacional-digesto-juridico-argentino

21 Mi explicación es más sencilla, pero claro es solo una opinión: simplemente en ese entonces los jueces y abogados con poder tenían más de 50 años y prefirieron un sistema contaminado pero que conocían a uno nuevo que sería rápidamente dominio de los jóvenes.

22 Martino, A. *Legislación y Digesto*, Eudeba, 2014.

23 https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/11.pdf

24 Los Congresos FAIDI, a partir de Santo Domingo han sido: Ciudad de Guatemala, Guatemala (1989), Mérida, España (1992), Bariloche, Argentina (1994), La Habana, Cuba (1996), Montevideo, Uruguay (1998), Lima, Perú (2000), México D. F., México (2000), San José, Costa Rica (2002), Santiago de Chile, Chile (2004), Ciudad de Panamá, Panamá (2006), Zaragoza, España (2008), Lima, Perú (2009), Monterrey, México (2010), Buenos Aires, Argentina (2011), Quito, Ecuador (2012), Santa Cruz, Bolivia (2013), San José, Costa Rica (2014), Medellín, Colombia (2015), Salamanca, España (2016), San Luis Potosí, México (2017), Ciudad de Panamá, Panamá (2018), San Pablo, Brasil (2019), Monterrey, México (2022), Villavicencio, Colombia (2023).

25 https://www.fiadi.org/

26 En Facebook tiene 1900 seguidores.

mática y derecho que ya cuenta con una segunda época[27], *Informática y Derecho, Revista Iberoamericana de Derecho Informático*, siendo la primera publicación periódica de habla castellana en derecho informático y que tiene además el valor de haber sido editada entre los 1992 y 2002 en 34 números y 7.549 páginas impresas. En la década que duró su existencia, participaron en ella los mejores expertos iberoamericanos en la materia, quienes la utilizaron no solo para publicar sus investigaciones y fortalecer la docencia universitaria, sino que sobre todo como un lugar de encuentro para debatir los temas que en cada momento eran de actualidad en el mundo del derecho y la informática y que ayudaron a los demás operadores del derecho a construir bases firmes para el desarrollo jurídico de la sociedad red. Además, está presente en YouTube, con *Somos la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI)*[28].

Es decir que la Revista FIADI ha contado y cuenta con especialistas en el tema y se ha ido actualizando a medida que han ido cambiando las tecnologías, contando con sus propios criterios de redacción[29]. En esta segunda etapa de la revista se ha realizado además la digitalización de todos sus números por el Instituto Chileno de Derecho y Tecnologías, a través de su presidente Carlos Reusser Monsálvez.

FIADI tiene también sus «fiadialogos» o libros FIADI, como el realizado el año pasado por Juan Carlos Sánchez entrevistando a Myrna Elia García Barrera, Marcelo Bauzá, Bibiana Luz Clara, Horacio Granero y Ramón Brenna.

Es posible también, pero lo pongo como interrogante, que como toda empresa internacional que se respete haya tenido sus reyertas internas, sus dificultades financieras y otros malestares que acosan a las entidades vivas. Solo les ruego que miren en el mapa la extensión de los países que participan, sus asociaciones, los medios sociales, su cultura, sus académicos y los medios judiciales involucrados y notarán que da vértigo. Ese vértigo que usted lector prueba, imagínelo en las autoridades que han debido afrontarlo a lo largo de cuatro décadas.

FIADI hasta tiene una «segunda época». «La Junta Directiva de lo que cabría denominar "segunda época de FIADI" se conforma durante el V Congreso (La Habana, 1996), y con algunas alternancias en su conformación ejerce funciones durante los siguientes 19 años (XIX Congreso, Medellín 2015)»[30].

Por Resolución n.º 634/2015 del 15 de diciembre de 2015, el Ministerio de Relaciones Exteriores de Uruguay le reconoce a FIADI su personería jurídica, a todos los efectos pertinentes. Se han revisado y actualizado los estatutos, por ejemplo, en 2015, y bajo la presidencia de Julio Alejandro Téllez Valdés, mexicano, y Patricia Reyes Olmedo, chilena, como secretaria, en Medellín, Colombia y ante el escribano Gastón Manug Agdjian[31].

27 https://www.derechoinformatico.cl/revista-fiadi/index.html

28 https://www.youtube.com/watch?v=GI5t3AsrVa0

29 https://fiadi.org/wp-content/uploads/2019/09/NORMAS-DE-PUBLICACION-REVISTA-FIADI.pdf

30 Cito de la historia de FIADI: https://www.fiadi.org/historia/

31 https://fiadi.org/wp-content/uploads/2016/05/estatutos.pdf

Ha publicado muchos libros, y hago mención solo de uno por su notable envergadura: *El derecho de las TIC en Iberoamerica*[32], en el 2019, con notables contribuciones desde Mario Losano hasta Michel Vivant, pasando por toda clase de especialistas iberoamericanos, con la dirección de Marcelo Bauzá Reilly. Probablemente es de los más completos sobre esta materia, con setenta y dos autores de los más destacados. Una obra que corta el aliento y que, para juzgarla, nada mejor que leerla, empezando con *FIADI, origen, evolución histórica, actualidad,* de Valentín Carrascosa López.

Sobre las personalidades de FIADI, es el tema más difícil porque seguramente voy a cometer enormes injusticias no nombrando a personas importantes, pero ya que me he arriesgado hasta aquí, ahí va la máxima osadía. Algunas de las personalidades a recordar son las que he nombrado en la parte anterior y me remito allí, para no repetir. Pero hay otras que no han sido nombradas siquiera y que deben ser recordadas.

Empecemos por Valentín Carrascosa. Si a Benito Roldan Casañé y Miguel López Muñiz Goñi se debe, en mayor medida, la fundación de FIADI, toda la etapa posterior es impensable sin este tesonero licenciado en la Universidad Complutense. Todo cuanto se pueda escribir sobre él es poco, por lo tanto, basta revisar la documentación de FIADI de estos ocho lustros para ver la recurrencia de Valentín en congresos, reuniones, promociones, acontecimientos, publicaciones.

Julio Téllez Valdés (México) y Juan Diego Castro (Costa Rica) son dos columnas en las se asentó FIADI, que fueran premiados con una membresía honoraria. Aparecen luego como en una saga iberoamericana: Federico Bueno, de España; Yarina Amoroso, de Cuba; Fernando Galindo, de España; Patricia Reyes, de Chile; Horacio Fernández Delpech, de Argentina; Pedro Patrón Bedoya, de Perú, José Heriberto García Peña (Cuba-México); Nelson Remolina Angarita, de Colombia; Ernesto Ibarra, de México; Marilina Rico Carrillo, de Estados Unidos; Elisa Palomino, de México, Natalia Darens Loreto, de Uruguay; Augusto Ho, de Panamá; Gustavo Amoni, de Venezuela; Humberto Martin Ruani y Daniel Ricardo Altmark, de Argentina, y tantos otros que no olvido, pero que se asoman en sus esfuerzos.

Y ahora el mundo nuevo en el cual le toca actuar. Cuando se creó FIADI, era la última parte de la civilización de la escritura y la imprenta de Gutenberg; esta en la cual vivimos es una era digital donde el predominio de la nueva tecnología presenta hasta clasificaciones etarias. La inteligencia artificial domina la escena desde armas autónomas, autos autogobernados, *fake news*, avatares que remplazan políticos y sistemas inteligentes que ordenan los vuelos. El tema es tan invasor que a los mesurados reclamos éticos de la Unesco[33] se está imponiendo la regulación más estricta[34].

32 Bauzá Reilly, M. (Dir.), *El derecho y las TIC en Iberoamérica,* La Ley, Uruguay, 2019.

33 En noviembre de 2021, la Unesco elaboró la primera norma mundial sobre la ética de la IA: la «Recomendación sobre la ética de la inteligencia artificial».

34 El 13 de marzo de 2024 el Parlamento Europeo aprobó la versión final de la *IA Act,* que tiene 180 considerandos, 13 capítulos, 113 artículos y 13 alegatos. Con un plan de vigencia que va desde los seis meses para aplicar los capítulos I y II, un año para la aplicación

Después de la pandemia, *mala tempora currunt* tanto en materia bélica, cuanto en ámbito económico, pero hay un escenario pujante y vibrante. En este nuevo mundo no me caben dudas de que FIADI seguirá con el espíritu de 1984, absolviendo su función en continuidad, lo que no es habitual en esta parte del mundo, con seriedad y con la parsimonia que le permitió llegar hasta aquí con fama y respeto. ¡Gloria y loor!

Bibiana Beatriz Luz Clara (Argentina), actual presidenta y su equipo, Ernesto Ibarra Sánchez (México), José Heriberto García Peña (Cuba/México), Julio Núñez Ponce (Perú) y Paulina Casares Subia (Ecuador), con una tarea difícil, pero provechosa y en buena sintonía con los tiempos que nos atraviesan, nos trasbordarán a ese tiempo nuevo.

de los capítulos III, V, VII y XI, dos años para que sean todos aplicables y treinta y seis meses para aplicar el art. 6, parágrafo 1.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 33-46

# EL REGLAMENTO EUROPEO *E-EVIDENCE* Y EL BALANCE ENTRE LA PROTECCIÓN DE DATOS Y LA SEGURIDAD TRANSFRONTERIZA

*THE EUROPEAN REGULATION ON E-EVIDENCE AND THE BALANCE BETWEEN DATA PROTECTION AND CROSS-BORDER SECURITY*

**Sarah Rachut**
**Julian W. Maurer**
TUM Center for Digital Public Services, Technical University of Munich (Alemania)

## Resumen

El presente artículo examina el Reglamento *E-Evidence*, adoptado por la Unión Europea en junio de 2023, el cual establece un marco legal para la cooperación transfronteriza en la obtención de pruebas electrónicas en investigaciones penales. Este reglamento surge de la necesidad de facilitar la obtención de pruebas almacenadas en el extranjero, especialmente en investigaciones relacionadas con terrorismo, fraude y delitos sexuales contra menores. El artículo revisa los antecedentes que llevaron a la creación del reglamento y muestra al lector una introducción en los dos instrumentos principales del nuevo Reglamento sobre la prueba electrónica: la Orden Europea de Producción y la Orden Europea de Conservación, permitiendo a las autoridades judiciales solicitar y preservar datos electrónicos de proveedores de servicios en otros Estados miembros de la UE.

Además, el artículo compara el Reglamento sobre la prueba electrónica con el *CLOUD Act* de Estados Unidos, destacando similitudes y diferencias, y analiza críticas, especialmente en cuanto a la protección de datos y la posible erosión de los derechos individuales. Se discute el impacto potencial del reglamento y la necesidad de seguimiento y evaluación continuos para prevenir abusos y garantizar el respeto a los principios del Estado de Derecho.



## Palabras clave

Prueba electrónica, regulación en la nube, protección de datos, delitos informáticos, tecnología.



## Abstract

This article examines the *E-Evidence* Regulation, adopted by the European Union in June 2023, which establishes a legal framework for cross-border cooperation in obtaining electronic evidence in criminal investigations. This regulation arises from the need to facilitate the collection of evidence stored abroad, especially in investigations related to terrorism, fraud, and sexual offences against children. The article reviews the background that led to the creation of the regulation and introduces the reader to the two main instruments of the new *E-Evidence* Regulation: the European Production Order and the European Preservation Order, allowing judicial authorities to request and preserve electronic data from service providers in other EU Member States.

In addition, the article compares the *E-Evidence* Regulation with the US CLOUD Act, highlighting similarities and differences, and analyses critics, especially in terms of data privacy issues and the potential erosion of individual rights. It also discusses the potential impact of the regulation and the need for continuous monitoring and evaluation to prevent abuses and ensure respect for rule of law principles.



## Keywords

*E-Evidence*, CLOUD Act, data protection, cybercrime, technology.

## Introducción

Las pruebas electrónicas tienen especial importancia en casi el 85 % de las investigaciones penales dentro de la Unión Europea, pero el 65 % de ellas suele obtenerse originariamente de otros países europeos distintos del Estado miembro investigador (Parlamento Europeo, 2023).

Especialmente en el contexto de las investigaciones antiterroristas, pero también en la persecución de fraude y de delitos sexuales contra menores. Asimismo, los investigadores de los Estados miembros precisan pruebas suficientemente completas y fiables. Sin embargo, a menudo estas pruebas se encuentran en el espacio digital y, por tanto, fuera del control de las autoridades policiales de los Estados miembros particulares, como España o Alemania. Con el *Reglamento sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (Reglamento E-Evidence* o *Reglamento sobre la prueba electrónica)* (Unión Europea, 2023b), la Unión Europea creó un marco jurídico para facilitar la cooperación transfronteriza entre las autoridades encargadas de la investigación penal y los proveedores de servicios que operan dentro de la Unión Europea, independientemente de si almacenan los datos de posibles sospechosos, sus usuarios, en servidores dentro o fuera de la Unión Europea.

El presente artículo esbozará principalmente los antecedentes y la historia del desarrollo del Reglamento sobre la prueba electrónica antes de pasar a explicar con más detalle los aspectos específicos del contenido normativo y los instrumentos concretos. A continuación se discutirá el Reglamento en el contexto del *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*) de los EE. UU. y se expondrán sus similitudes y diferencias antes de formular una serie de críticas.

## Antecedentes y trayectoria del Reglamento *E-Evidence*

Debido al surgimiento del terrorismo islamista en el plano internacional, en el que se lleva viviendo desde hace ya más de una década, los ministros de justicia de la Unión Europea acordaron ya en marzo de 2016 dar prioridad a la creación de medidas para la obtención y la seguridad eficientes y eficaces de las pruebas electrónicas en el futuro. Estas deliberaciones vinieron precedidas, entre otros, por los atentados terroristas de París del 13 de noviembre de 2015, y los atentados terroristas de Niza del 14 de julio de 2016, de Berlín del 19 de diciembre de 2016 y, finalmente, de Barcelona del 17 de agosto de 2017 hicieron que el tema cobrara aún más relevancia (López Werner, 2023; Pacelli, 2023; Andreeva, 2020). En los atentados mencionados, los autores se habían comunicado en una medida nada desdeñable a través de canales de comunicación en línea en el período previo al delito y durante el mismo.

En un dictamen emitido por el Consejo de Justicia y Asuntos de Interior de la Unión Europea el 9 de junio de 2016, el Consejo concluyó, entre otras constataciones, que debe negarse a toda costa a los actores delictivos un «refugio seguro» en el ciberespacio y que será necesario actuar ante el creciente impacto de la

ciberdelincuencia como tal, pero también debido a las actividades delictivas que posibilita internet en general (Consejo de la Unión Europea, 2016). En concreto, el Consejo destacó la importancia de las pruebas electrónicas en los procesos penales, razón por la cual las autoridades policiales y judiciales de los Estados miembros deben estar dotadas de herramientas completas y eficaces para investigar y perseguir los delitos relacionados con el ciberespacio. En particular, el Consejo sugirió que se ampliara la cooperación entre los proveedores y las autoridades de seguridad. Con ello se agilizarán los procedimientos de asistencia judicial y se revisará la normativa relativa a la aplicación de la ley en el ciberespacio. Entre diciembre de 2016 y junio de 2017, los servicios de la Comisión publicaron otros documentos de trabajo, y este último documento, publicado el 8 de junio de 2017, también contenía propuestas de medidas sobre cómo mejorar específicamente el acceso a los documentos digitales y a la información en las investigaciones penales transfronterizas (Comission Services, 2017; Burchard, 2018).

Finalmente, las propuestas desarrolladas por la Comisión dieron lugar en 2018 al proyecto de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (Reglamento *E-Evidence*), que la Comisión Europea presentó el 18 de abril de 2018. El Parlamento Europeo aprobó finalmente la propuesta ligeramente modificada el 13 de junio de 2023. Además del Reglamento sobre la prueba electrónica, se adoptó el 12 de julio de 2023, como parte del paquete *E-Evidence*, la llamada Directiva de Representantes (Unión Europea, 2023a), que regula la designación de sucursales y el nombramiento de representantes de determinados proveedores de servicios. Para facilitar la aplicación del Reglamento sobre la prueba electrónica, estos proveedores de servicios deberán designar representantes o establecimientos dentro de la Unión Europea encargados de recibir, cumplir y hacer cumplir las decisiones y órdenes emitidas por las autoridades de investigación.

## Disposiciones e instrumentos del Reglamento *E-Evidence*

El núcleo del Reglamento sobre la prueba electrónica adoptado es la introducción de los instrumentos de una *Orden Europea de Producción* y una *Orden Europea de Conservación*, en virtud de los cuales estas deben ser expedidas o validadas por la autoridad judicial competente de un Estado miembro en su aplicación específica según la propuesta. El art. 3 n.º 1 del Reglamento *E-Evidence* define la *Orden Europea de Producción* como

> una decisión por la que se ordena la entrega de pruebas electrónicas, emitida o validada por una autoridad judicial de un Estado miembro (…), y dirigida a un establecimiento designado o a un representante legal de un prestador de servicios que ofrezca servicios en la Unión, cuando dicho establecimiento designado o representante legal esté situado en otro Estado miembro (…).

La *Orden Europea de Conservación*, por su parte, se define como

> una decisión por la que se ordena la conservación de pruebas electrónicas a los efectos de una solicitud posterior de entrega, y que es emitida o validada por una autoridad judicial de un Estado miembro (…), y dirigida a un establecimiento designado o a un representante legal de un prestador de servicios que ofrezca servicios en la Unión, cuando dicho establecimiento designado o representante legal esté situado en otro Estado miembro (…). (Art. 3, num. 2 del Reglamento *E-Evidence*).

Estas órdenes deben aplicarse en particular cuando los datos hayan sido almacenados por un proveedor de servicios de otro país, y puedan a su vez ser relevantes como prueba en el contexto de investigaciones o procesos penales. De conformidad con el art. 3, num. 3 del Reglamento *E-Evidence*, los proveedores de servicios son aquellas personas físicas o jurídicas que ofrecen uno de los servicios definidos con en el art. 3, num. 2, lits. *a* a *c* (incluidos servicios de comunicaciones electrónicas, servicios de nombre de dominio de internet y de direcciones IP, tales como asignación de direcciones IP, registro de nombres de dominio, registrador de nombres de dominio y servicios de privacidad y representación relacionados con nombres de dominio y otros servicios de la sociedad de la información). En este contexto, debe tenerse en cuenta que la ejecución de una Orden Europea de Producción o de Conservación solo será admisible en la proporción en que sería posible adoptar una medida similar en una situación hipotética comparable en el territorio nacional del Estado de emisión. En este contexto, cabe señalar también que el Reglamento sobre la prueba electrónica no contempla ninguna medida específica de vigilancia, ni siquiera incluye normas sobre la retención de metadatos. El objetivo del reglamento se centra más bien en la facilitación de la labor de la autoridad de instrucción penal en la fase de investigación y enjuiciamiento en cada caso concreto, por lo que el ámbito de aplicación de los instrumentos previstos se extiende exclusivamente a las fases que abarcan desde la investigación previa al juicio hasta la respectiva resolución del procedimiento por archivo o sentencia. La entrega de datos de abonado y de acceso puede solicitarse en todas las diligencias penales, mientras que la entrega de datos de transacción y de contenido solo se permite cuando se trata de delitos punibles en el Estado de emisión con una pena privativa de libertad mínima de tres años (véase el artículo 5.3 y 5.4 lit. *a* del Reglamento *E-Evidence*).

Las excepciones son los actos delictivos ya señalados explícitamente en la propuesta legislativa, cuando pueda establecerse un vínculo suficiente entre el uso de los sistemas de información y el hecho delictivo en cuestión (en particular en materia de lucha contra el fraude y la falsificación en relación con los medios de pago distintos del efectivo, los abusos sexuales y la explotación sexual de menores y la pornografía infantil, así como los ataques contra los sistemas informáticos; véase el artículo 5.4, lit. *b*, del Reglamento *E-Evidence*) o los delitos que entran en el ámbito de aplicación de la Directiva de la Unión Europea (2017) relativa a la lucha contra el terrorismo (artículo 5.4, lit. *c*, del Reglamento *E-Evidence*).

En cuanto a la ejecución de una Orden Europea de Producción, el Reglamento *E-Evidence* establece que los datos solicitados deben transmitirse a la autoridad de emisión o a la autoridad fiscal competente en un plazo máximo

de diez días a partir de la recepción de la orden, aunque en casos excepcionales podría ser conveniente tramitarlos antes (art. 9.1 del Reglamento *E-Evidence*). En casos de emergencia, los datos solicitados deben tramitarlos incluso inmediatamente, pero a más tardar en un plazo de seis horas a partir de la recepción de la orden (art. 9.2 del Reglamento *E-Evidence*). En el caso de las órdenes de mera conservación, los datos solicitados deben conservarse inmediatamente de conformidad con el artículo 10.1, del Reglamento *E-Evidence*, según el cual esta conservación finaliza a los sesenta días, a menos que la autoridad emisora confirme al proveedor de servicios que se ha iniciado una solicitud de entrega. En tal caso, el proveedor de servicios deberá conservar los datos durante el tiempo necesario para entregarlos tras la recepción de la solicitud de entrega (art. 10.2 del Reglamento *E-Evidence*). Por lo tanto, en el sistema de órdenes, la Orden Europea de Conservación sólo sirve para preservar datos para ocasiones específicas, cuya entrega podría ordenarse posteriormente en el curso ulterior del procedimiento. Tras la solicitud de una autoridad, existen por lo general tres escenarios posibles: En el mejor de los casos, el proveedor de servicios coopera y transmite los datos a la autoridad de ejecución, que a su vez los transmite a la autoridad solicitante (Magno, 2023, p. 26). Si el proveedor de servicios rechaza la solicitud, los motivos deben ser evaluados por la autoridad de ejecución, que entonces ejecuta la orden o pide más información a la autoridad de origen. En caso de que la autoridad de ejecución llegara a la conclusión de que la orden no puede ejecutarse, deberá ponerse en contacto con la autoridad de origen (Magno, 2023, p. 26).

## Los procedimientos de investigación criminal y la protección de datos

Incluso antes de la entrada en vigor del Reglamento *E-Evidence*, las cuestiones de seguridad y protección de datos no eran en absoluto irrelevantes en el contexto de los procedimientos de obtención de pruebas. De hecho, en el marco de las investigaciones policiales y fiscales también se procesan regularmente datos personales. En general, los datos personales están sujetos a la protección especial del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos, RGPD) (Unión Europea, 2016). En definitiva, el RGPD entiende como datos personales cualquier información sobre una persona física identificada o identificable. Asimismo, se considera como persona física identificable

> toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. (Art. 4.1 RGPD).

Con respecto al tratamiento de datos personales, se entiende como tal

> cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. (Art. 4.2 RGPD).

Sin embargo, debe tenerse en cuenta que la aplicabilidad del RGPD a los datos personales obtenidos durante las investigaciones penales debe excluirse de manera coherente. Esto también se desprende claramente del mismo Considerando n.º 19 del RGPD, que señala que las disposiciones del RGPD no son aplicables a las investigaciones penales. De lo contrario, sería inconcebible una labor de investigación significativa y eficaz. La protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección y la prevención de amenazas para la seguridad pública, y la libre circulación de dichos datos se regulan, por tanto, en un instrumento independiente de la legislación europea (Considerando n.º 19, apartado 1, frase 1). Por lo tanto, el RGPD no se aplicará explícitamente a las actividades de tratamiento con fines de investigación (Considerando n.º 19, apartado 1, frase 2).

Sin embargo, debido a la creciente relevancia de conductas delictivas cibernéticas vistas en los últimos años, el solapamiento entre las actividades de investigación de las autoridades y la participación de entidades privadas en los procedimientos de investigación es cada vez mayor. En una época en la que gran parte de la vida de los ciudadanos de la Unión Europea transcurre en el espacio digital y en la que las posibilidades de conservación de datos (sin autorización previa) están justamente restringidas, resulta cada vez más difícil distinguir entre la gestión de datos de carácter puramente oficial y la de carácter privado. Ello también se manifiesta en la práctica en las cadenas de cooperación de intervinientes privados, por ejemplo las grandes empresas tecnológicas, por un lado, y los investigadores públicos, por otro (Robinson, 2023, p. 2). No obstante, diversas formas y niveles de tratamiento de datos se ven afectados por esta circunstancia.

## El Reglamento *E-Evidence* en el contexto de las iniciativas transatlánticas

Se puede contemplar la *CLOUD Act* estadounidense como el homólogo transatlántico del Reglamento sobre la prueba electrónica (US Department of Justice, 2018; Abraha, 2020, pp. 324-325).

Así pues, con el *CLOUD Act* a un lado del Atlántico y el Reglamento *E-Evidence* al otro, se enfrentarán dos actos jurídicos con una orientación similar, pero marcos jurídicos diferentes.

De hecho, el planteamiento de la Unión Europea va algo más lejos que el homólogo estadounidense del Reglamento sobre la evidencia electrónica. Mientras

que el *CLOUD Act* únicamente estipula que los proveedores de servicios estadounidenses están obligados a revelar los datos almacenados en caso de solicitud de revelación por parte de las autoridades de los EE. UU., incluso si se encuentran en un servidor fuera del país, el Reglamento *E-Evidence* establece que los proveedores de servicios deben revelar siempre los datos en cuestión, sin diferenciar dónde y quién los almacena. Esta obligación de información se aplica íntegramente a todos los proveedores de servicios que operan en la Unión Europea, independientemente de que sean o no empresas originariamente europeas. Por tanto, la obligación de revelar datos a las autoridades de los Estados miembros europeos también afectará a las empresas estadounidenses que no almacenen sus datos en Europa y les planteará nuevos retos en materia de protección de datos. En este sentido, para ellos, el potencial de conflicto en el marco de la legislación estadounidense de protección de datos surge del hecho de que, por regla general, las empresas estadounidenses no están autorizadas a entregar a las autoridades policiales de otros países datos sobre contenidos almacenados en EE. UU[1]. En consecuencia, las empresas estadounidenses se verán obligadas a incurrir en conductas prohibidas por la normativa de su país de origen. Este problema de protección de datos, que limitaría considerablemente la eficacia del Reglamento *E-Evidence* debido a su gran importancia, sólo podrá resolverse en última instancia mediante acuerdos correspondientes entre la UE y EE. UU. Sin embargo, es de suponer que una flexibilización de las correspondientes disposiciones de protección de datos de EE. UU. posiblemente se traduciría en un alto coste para el mismo, en términos de protección de datos por parte de la UE.

## Crítica

Cuando se publicó por primera vez la versión del proyecto en 2018, la Comisión Europea ya se vio sometida a un amplio abanico de críticas, que desde entonces ya se habían suavizado. Sin embargo, a más tardar desde que se alcanzó el acuerdo político entre el Consejo Europeo y el Parlamento en enero de 2023, que en última instancia condujo a la adopción del Reglamento *E-Evidence* en el Parlamento Europeo el 13 de junio de 2023, el asunto ha vuelto a estar de actualidad.

El nuevo reglamento ha sido criticado, en particular, por cuestiones relacionadas con la protección de datos. Sin embargo, algunas otras disposiciones también son cuestionables a la luz del deterioro de la calidad del Estado de Derecho en algunos Estados miembros. Esto se aplica en particular al acceso a los datos de tráfico de internet, que pueden permitir sacar conclusiones precisas sobre la vida (privada) de una persona —siendo este último un peligro especialmente importante[2]—. A la vista de las enseñanzas extraídas del escándalo de las escuchas telefónicas *Pegasus*, en el que se reveló que Hungría, Polonia, España y Grecia, entre otros países, espiaban a ciudadanos políticamente indeseables (Raebisch, 2024, p. 65), puede criticarse sin duda una posibilidad exageradamente sencilla de acceso transnacional a datos sensibles.

1 *Vid*. también: Meissner (2023).

2 *Vid*. en este contexto también: Oromí i Vall-Llovera (2020).

Un cambio significativo, que también se debe en gran medida al debate crítico del primer borrador de la Comisión de 2018, se puede ver en el establecimiento del requisito de notificación del art. 13.1 del Reglamento *E-Evidence*, según el cual el interesado sobre el que se han solicitado los datos debe ser informado inmediatamente (De Hoyos Sancho, 2020, p. 108; Muriel Diéguez, 2024, p. 190). Únicamente se contemplan excepciones en los casos en que la notificación no parezca adecuada por razones de salvaguardia de las investigaciones o de protección de la seguridad nacional (art. 13.2 del Reglamento sobre la prueba electrónica).

Desde el punto de vista de la política jurídica, también resulta cuestionable hasta qué punto el Reglamento *E-Evidence* puede tener un efecto de modelo negativo. Con razón se apunta que el Reglamento podría servir de «modelo» para que los Estados no pertenecientes a la UE introduzcan normativas similares y que los Estados miembros de la UE podrían verse confrontados con órdenes de entrega que contribuirían a la persecución de delitos muy alejados de nuestras tradiciones jurídicas.

En este contexto, también hay que hacer especial referencia a las preocupaciones de la Conferencia Alemana de Protección de Datos, aún en relación con la actualmente suspendida legislación sobre conservación de metadatos en Alemania, que ya se expresaron en la fase de proyecto[3]. Estas son sumamente comprensibles, sobre todo teniendo en cuenta el pasado de Alemania y la fuerte brújula moral resultante, que hoy en día se refleja sobre todo en la defensa de los derechos humanos en todo el mundo. En particular, debido al deterioro de la calidad del Estado de Derecho en España (Hay Derecho, 2023) y algunos países de la Unión Europea (Gora y De Wilde, 2020), así como los recientes acontecimientos en España (por ejemplo, las circunstancias democráticamente cuestionables de la amnistía para los delincuentes separatistas catalanes (Ruíz Bursón, 2023, pp. 83, 122) o la falta de independencia política de la fiscalía y las autoridades de investigación españolas (Martínez Santos, 2022; Villoria Mendieta, 2022)), es preciso seguir de cerca la evolución y la aplicación del Reglamento *E-Evidence*. Especialmente porque, sobre todo en España, los supuestos delitos de responsables políticos o sus familiares a menudo se ven utilizados deliberadamente por corrientes políticas opuestas para debilitar a la oposición.

3 *Vid*.: «Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u.a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten» («Sin embargo, resulta especialmente importante que los proveedores de servicios de telecomunicaciones en Alemania estén obligados, entre otras cosas, a almacenar todos los datos de tráfico durante diez semanas. Estos datos pueden utilizarse para extraer conclusiones precisas sobre la vida privada de los afectados, en particular sus perfiles de contactos e intereses. El problema de esta retención de metadatos se agrava considerablemente si autoridades policiales extranjeras también obtienen acceso directo a dicha información») (Datenschutzkonferenz, 2018).

Recientemente conocimos un ejemplo actual: tras destaparse el escándalo de presunta corrupción del secretario de organización del PSOE y ministro de Fomento, así como de Transportes, Movilidad y Agenda Urbana, José Luis *Ábalos* Meco (Miranda, 2024; Alonso, 2024), la ministra de Hacienda y vicepresidenta primera del gobierno, María Jesús Montero Cuadrado (PSOE) utilizó en el debate público las especulaciones sobre supuestas faltas fiscales de la pareja de la presidenta de la Comunidad de Madrid, Isabel Díaz Ayuso (PP), para desviar el foco de atención del PSOE (Benito, 2024; Sarriá, 2024; García, 2024). Se trataba de una información que la ministra no estaba legalmente autorizada a disponer ni a publicar. Es fácil imaginar los peligros que entraña la normativa sobre pruebas electrónicas, sobre todo para los países que se están alejando cada vez más de los principios democráticos.

## Algunas consideraciones finales

La persecución de delincuentes en el espacio digital es una importante cuestión de interés. En particular, ahora que internet y los canales de comunicación asociados desempeñan un papel cada vez más importante en la preparación, ejecución y seguimiento de delitos violentos y actos de terrorismo en todo el mundo, las autoridades policiales y judiciales deben disponer de herramientas eficaces y eficientes para proteger la seguridad de todos nosotros de la mejor manera posible. Al mismo tiempo, deben defenderse los principios del Estado de Derecho. Existe, por tanto, un conflicto de objetivos entre la seguridad absoluta de los derechos individuales de los presuntos delincuentes y los del resto de la población, que debe ser protegida por el Estado de Derecho. En consecuencia, este conflicto de objetivos, esta zona de tensión, debe conciliarse de la mejor manera posible, y si esto se logrará con el Reglamento *E-Evidence* está por ver y dependerá también en gran medida de cómo utilicen las autoridades policiales y judiciales de los Estados miembros las nuevas posibilidades y en qué dirección se desarrollen las negociaciones entre la UE y los EE. UU. Lo que sí es seguro es que la aplicación del Reglamento *E-Evidence* debe ir acompañada de un proceso de evaluación crítica. En la medida de lo posible, debe evitarse el uso indebido de las competencias y, en caso de duda, el reglamento debe corregirse a tiempo.

## Referencias bibliográficas

Abraha, H. (2020). Regulating law enforcement access to electronic evidence across borders: the United States approach. *Information & Communication Technology Law* (3), 324-353.

Alonso, M. (2024). Ábalos, el leal sanchista caído en desgracia. *ABC España*. https://www.abc.es/espana/abalos-leal-sanchista-caido-desgracia-20240225172744-nt.html.

Andreeva, C. (2020). The EU's counter-terrorism policy after 2015 — «Europe wasn't ready» — «but it has proven that it's adaptable». *ERA Forum* (20), 343-370.

Benito, M. (2024). La pareja de Ayuso se querellará contra la ministra Montero. *La Razón*. https://www.larazon.es/madrid/pareja-ayuso-querellara-ministra-montero_2024031565f44301ab79d80001a570a2.html.

Burchard, C. (2018). Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1. *Zeitschrift für Internationale Strafrechtsdogmatik* (6), 190-203.

Commission Services. (2017). *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*. https://era-comm.eu/EPPO/kiosk/pdf/Non_paper_Improving_cross_border_access_electronic_evidence.pdf.

Consejo de la Unión Europea. (2016). *Council conclusions on improving criminal justice in cyberspace*. https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.

Datenschutzkonferenz. (2018). *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7.* https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20181107_EntschliessungE_Evidence.pdf?__blob=publicationFile&v=7.

De Hoyos Sancho, M. (2020). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo. *Revista de Estudios Europeos* (1-extra), 99-128.

García, C. (2024). El PP denuncia las maniobras del sanchismo para desviar a Madrid la atención del «caso Koldo». *La Razón*. https://www.larazon.es/madrid/denuncia-maniobras-sanchismo-desviar-madrid-atencion-caso-koldo_2024030265e289ca566e5f00019e99f2.html.

Gora, A., De Wilde, P. (2020). The essence of democratic backsliding in the European Union: deliberation and rule of law. *Journal of European Public Policy* (2), 342-362.

Hay Derecho. (2023). *Situación del Estado de Derecho en España 2023*. https://www.hayderecho.com/wp-content/uploads/2023/12/Situacion-Estado-de-Derecho-Espana-2023.pdf.

López Werner, E. (2023). La exportación del terrorismo a través de Emni: un repaso de los atentados desde Siria hasta Libia, instrumentados bajo la marca del servicio de operaciones exteriores de Estado Islámico entre 2014 y 2017. *Revista del Instituto Español de Estudios Estratégicos* (21), c139-167.

Magno, T. (2023). The Challenging Path Towards the Establishment of the EU Legal Framework Regulating Cross-Border Access to Digital Evidence. En A. Biasiotti, F. Turchi (Coords.), *European Investigation Order* (23-33).

Martínez Santos, A. (2022). Emisión de órdenes europeas de investigación por el Ministerio Fiscal español. Consideraciones sobre la compatibilidad del art. 13.4 de la Ley de reconocimiento mutuo con el derecho de la Unión a la luz de las Sentencias del TJUE en los Asuntos Gavanozov I y II. *Revista General de Derecho Europeo* (57), 272-317.

Meissner, P. (2023). Digitale Beweise im EU-/US-Datenschutzkonflikt. *Verfassungsblog*. https://verfassungsblog.de/digitale-beweise-im-eu-us-datenschutzkonflikt/.

Miranda, B., (2024). José Luis Ábalos: simpático, mujeriego y prolífico. *El Mundo*. https://www.elmundo.es/loc/famosos/2024/02/22/65d729e5fc6c83fe068b4596.html.

Muriel Diéguez, J. (2024). Las Órdenes de Entrega y Conservación de Pruebas Electrónicas en el Proceso Penal Europeo. *Revista de Estudios Europeos* (83), 172-201.

Oromí i Vall-Llovera, S. (2020). Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE. *Revista de Internet, Derecho y Política* (31), 1-13.

Pacelli, D. (2023). El papel del miedo en los fenómenos colectivos: El miedo a los demás y la necesidad de la sociedad entre la política y la información. *Comunicación y Hombre* (19), 27-38.

Parlamento Europeo. (2023). *Electronic evidence: new rules to speed up cross-border criminal investigations*. https://www.europarl.europa.eu/news/es/press-room/20230609IPR96203/electronic-evidence-new-rules-to-speed-up-cross-border-criminal-investigations.

Raebisch, M. (2024). Pegasus: análisis de su impacto en los derechos fundamentales en Europa. *Quaderns IEE: Revista de l'Institut d'Estudis Europeus* (1), 62-87.

Robinson, G. (2023). Like Oil and Water? Effective Data Protection and Direct Cooperation on Digital Evidence. En V. Franssen, S. Tosza (Coords.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (1-35). Cambridge.

Ruíz Bursón, F. (2023). ¿Es constitucional una ley de amnistía? Estado actual de la cuestión: argumentos a favor y en contra. *Corts. Anuari de Dret Parlamentari* (37), 83-127.

Sarriá, B. (2024). Génova respalda a Ayuso ante el señalamiento del PSOE por las cuentas de su pareja: «No afecta al PP». *20minutos*. https://www.20minutos.es/noticia/5227072/0/genova-respalda-ayuso-ante-senalamiento-psoe-por-las-cuentas-su-novio-no-afecta-pp/.

Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679.

Unión Europea. (2017). *Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se*

*modifica la Decisión 2005/671/JAI del Consejo.* https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32017L0541.

Unión Europea. (2023a). *Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023L1544.

Unión Europea. (2023b). *Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R1543.

US Department of Justice. (2018). *Clarifying Lawful Overseas Use of Data Act.* https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf.

Villoria Mendieta, M. (2022). Un análisis comparado de la lucha contra la corrupción en Europa, con especial referencia a España. *Revista Española de Control Externo* (72) 10-35.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 47-56

# ESTATUTO JURÍDICO DE LOS PROVEEDORES DE SERVICIOS DE INTERMEDIACIÓN EN LÍNEA EN EL REGLAMENTO EUROPEO SOBRE PLATAFORMAS DIGITALES

*LEGAL STATUS OF ONLINE INTERMEDIATION SERVICE PROVIDERS IN THE EUROPEAN REGULATION ON DIGITAL PLATFORMS*

**Mariliana Rico Carrillo**

Catedrática de Derecho Mercantil, Universidad Católica del Táchira (Venezuela)

## Resumen

El Reglamento europeo sobre plataformas digitales (P2B) entró en vigor el 12 de julio de 2020. Es el primer marco general aplicable a los servicios de intermediación en línea. Estos servicios son intermediarios para un gran número de empresas grandes y pequeñas, o «usuarios empresariales», dentro del mercado interior. Esta norma establece las obligaciones de los proveedores de servicios de intermediación en línea respecto a la incorporación de condiciones generales de contratación y sus deberes de transparencia en sus relaciones con las empresas y los usuarios profesionales. La finalidad de este artículo se centra en el estudio de forma y el contenido que deben cumplir estas condiciones con la finalidad de lograr una competencia leal en los mercados digitales.



## Palabras clave

Proveedores de servicios de intermediación en línea, plataformas digitales, condiciones generales de contratación, empresarios y usuarios profesionales.



## Abstract

The European Regulation on digital platform services (P2B) is in effect since July 12, 2020. It is the first general framework applicable to online intermediation services. These services intermediate for a considerable number of large and small companies, or 'business users', within the internal market. This regulation establishes obligations of online intermediation service providers regarding to the incorporation of general contracting conditions and their duties of transparency in their relationships with business users. This paper focuses on the study of the form and content that these conditions must meet in order to achieve fair competition in digital markets.



## Keywords

Online intermediation service providers, digital platforms, general contract conditions, entrepreneurs, business users.

## Introducción

En julio de 2020 entró en vigor el Reglamento UE 2019/1150 del Parlamento Europeo y del Consejo, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, conocido como «Reglamento sobre plataformas digitales y empresas» o simplemente «Reglamento P2B» (*Platform to Business*). La finalidad de esta norma se centra en establecer un equilibrio en las relaciones entre el titular de la plataforma (proveedor de servicios de intermediación en línea) y los empresarios profesionales alojados en ella, mediante la introducción de la regulación aplicable a las condiciones generales que rigen la relación entre estos sujetos, y el establecimiento de los correspondientes deberes de transparencia. Las ventajas de la aprobación de este reglamento son significativas para todos los sectores de la economía. La transparencia en las plataformas en línea y la confianza en las relaciones empresariales no solo beneficia a las empresas sino que además repercute en la confianza de los consumidores y en la consolidación de los mercados digitales.

Aunque el Reglamento P2B es europeo, su entrada en vigencia tiene importantes implicaciones a nivel internacional, ya que su ámbito de aplicación es suficientemente amplio como para cubrir las empresas con domicilio legal fuera del territorio de la Unión Europea. Urgía ya la necesidad de contar con una norma de esta naturaleza ante las numerosas prácticas abusivas de las grandes empresas tecnológicas como Google, Amazon o eBay, derivadas de su posición de dominio en el mercado en detrimento de las empresas alojadas en las distintas plataformas digitales (Rico Carrillo, 2002).

## Análisis del reglamento europeo sobre plataformas digitales

### 1. Finalidad y ámbito de aplicación

El Reglamento P2B se aplica fundamentalmente a las plataformas de servicios de intermediación (*e-marketplaces,* tiendas de aplicaciones y redes sociales) y a los motores de búsqueda como Google. Su finalidad es contribuir al correcto funcionamiento del mercado interior mediante el establecimiento de normas para asegurar que se conceden opciones apropiadas de transparencia, de equidad y de reclamación a los usuarios profesionales de servicios de intermediación en línea, tal como lo dispone el artículo 1.1.

El artículo 1.2 es específico al indicar que se aplicará a dos grupos de servicios: a) los servicios de intermediación en línea, y b) los servicios de motores de búsqueda. En esta oportunidad me centraré en los servicios de intermediación, ya que los servicios de motores de búsqueda han sido objeto de estudios previos (Rico Carrillo, 2002). Los proveedores de estos servicios, denominados en general proveedores de servicios de intermediación en línea (PSIL) están sometidos al Reglamento P2B siempre que tengan su lugar de establecimiento o domicilio en la UE, sin embargo y como indicamos en la parte introductoria, también se aplica a aquellos PISL que ofrezcan bienes o servicios a los consumidores ubicados en el territorio de la UE, con independencia de dónde estén establecidos o residan estos proveedores y cualquiera que fuese la ley aplicable.

La redacción de este precepto tiene importantes implicaciones a nivel internacional, ya que su ámbito de aplicación es suficientemente amplio como para cubrir las empresas con domicilio legal fuera del territorio de la UE, como es el caso de grandes plataformas como Amazon, Google, Facebook, Apple y Yahoo, entre otras.

## 2. Definiciones relevantes

Las definiciones relevantes se encuentran delimitadas en el artículo 2 del Reglamento P2B. A efectos de este trabajo es importante tener presentes tres:

*1) Servicios de intermediación en línea.* Son los servicios de la sociedad de la información que permiten a los usuarios profesionales ofrecer bienes y/o servicios a los consumidores, con el objetivo de facilitar el inicio de transacciones directas entre dichos usuarios profesionales y consumidores, con independencia de dónde aquellas concluyan en última instancia. Estos servicios se prestan sobre la base de relaciones contractuales entre el proveedor de los servicios y los usuarios profesionales que ofrecen los bienes o servicios a los consumidores. En el caso de las plataformas de comercio electrónico como Amazon o eBay, la característica principal de estos servicios es la intermediación, que permite que las partes se pongan en contacto para facilitar el inicio de transacciones directas entre las empresas o los profesionales alojados en la plataforma y los consumidores. Como ya se indicó, esta definición incluye las plataformas de comercio electrónico (*e-marketplaces*), las tiendas de aplicaciones y las redes sociales.

*2) Usuarios profesionales.* Esta categoría de sujetos es definida en forma amplia como todo particular que actúa en el marco de una actividad comercial o profesional o una persona jurídica que ofrece bienes o servicios a los consumidores relacionados el comercio, oficio o profesión. En el marco de este concepto se diferencian claramente dos sujetos: las empresas comerciales y los profesionales que prestan servicios en los mercados electrónicos.

*3) Condiciones generales de contratación.* Son todas cláusulas que rigen la relación entre los PSIL y los usuarios profesionales, que son determinadas unilateralmente por el proveedor de los servicios en línea. El elemento más importante de esta definición es la determinación unilateral de las condiciones que van a regir el contrato. La posición de superioridad de los PSIL, la ausencia de una regulación especifica y la imposibilidad de la negociación fueron los tres elementos que provocaron la redacción de cláusulas abusivas en el sector de las plataformas y, en consecuencia las correspondientes denuncias ante las autoridades de la competencia y las correspondientes demandas.

## 3. Normas que rigen las condiciones generales de contratación (CGC)

### *3.1. Condiciones de forma*

El artículo 3 del Reglamento P2B establece la forma y el contenido que deben cumplir las CGC, incluyendo las reglas sobre modificación de las condiciones, resolución del contrato y nulidad de las cláusulas.

Las CGC deben redactarse en forma clara y sencilla y estar disponibles en todas las etapas de la relación contractual, incluyendo la fase previa a la celebración del contrato. La información precontractual es importante para que los futuros usuarios de la plataforma conozcan las condiciones de funcionamiento y decidan si les conviene o no contratar el servicio. En cuanto a su contenido, deben estipular las razones en las que se basan las decisiones de suspender, terminar o restringir —de manera total o parcial— la prestación de los servicios de intermediación en línea a los usuarios profesionales e incluir la información sobre los canales de distribución adicionales, así como los posibles programas a través de los cuales el PSIL podría comercializar los bienes o servicios ofrecidos por los usuarios profesionales.

Las cláusulas que no cumplan estas condiciones se considerarán nulas. Aquí deben aplicarse los principios tradicionales del derecho contractual y en particular del derecho de consumo que disponen que la nulidad solo afecta a la cláusula en cuestión y no a la integridad del contrato. A tal efecto, el considerando 20 indica las condiciones generales que no cumplan la normativa deben ser nulas de pleno derecho, esto es, se debe considerar que nunca han existido, con efectos *erga omnes* y *ex tunc*. Esto solo debe afectar a las cláusulas específicas de las CGC que no cumplan la normativa. Las otras cláusulas deben seguir siendo válidas y aplicables en la medida en que se puedan disociar de las cláusulas que no respeten la normativa.

### *3.2. Condiciones de modificación*

Cualquier propuesta de modificación debe ser notificada a los usuarios profesionales antes su aplicación. El artículo 3.2 dispone que la comunicación de esta notificación debe hacerse en un soporte duradero y en un plazo razonable y proporcionado (al menos quince días antes de la fecha en que el PSIL comunique a los usuarios profesionales afectados las modificaciones propuestas). El concepto de soporte duradero lo encontramos en el artículo 2 del Reglamento P2B y es definido como todo medio que permita a los usuarios profesionales almacenar información que se les transmita personalmente de forma que esté accesible para futuras consultas y durante un período de tiempo acorde con los fines de dicha información y que permita la reproducción de la información almacenada sin cambios.

### *3.3. Tratamiento diferenciado*

A efectos de evitar prácticas de competencia desleal, el artículo 7 regula los supuestos en que los PSIL u otros profesionales usuarios bajo su control actúan como proveedores de bienes o servicios.

De acuerdo con el artículo 7.1, los PSIL tienen el deber de incluir en sus CGC una descripción de todo trato diferenciado que den o puedan dar, en relación con los bienes o servicios que esos mismos proveedores u otros usuarios profesionales que estén bajo su control ofrezcan a los consumidores en relación con otros usuarios profesionales. En esa descripción se mencionarán las principales

consideraciones económicas, comerciales o jurídicas que fundamentan el trato diferenciado.

Esta disposición establece en detalle todos los aspectos que debe incluir la descripción. La finalidad de este precepto es brindar transparencia en los sistemas de clasificación, de modo que los usuarios de la plataforma —tanto los empresarios como los consumidores— tengan conocimiento de cualquier trato diferenciado que se preste, bien sea al PSIL o a las empresas bajo su control.

### *3.4. Protección de datos*

El tratamiento de datos es relevante —y muy controvertido— en el mercado de las plataformas, de ahí la necesidad de incluir este aspecto en la regulación sectorial de los servicios de intermediación en línea. Para usar los servicios de un PSIL es necesario que tanto los usuarios profesionales como los consumidores faciliten información. Este modelo negocio se centra básicamente en la captación y el tratamiento de datos de sus usuarios (tanto de las empresas como de los consumidores), ya que esta información es la que les permite llegar con mayor facilidad al consumidor final.

La información de los empresarios y los consumidores incide directamente en el éxito comercial tanto del PSIL como de las empresas alojadas en su plataforma. Tomando en cuenta estas circunstancias, el legislador comunitario introduce en el artículo 9 las normas sobre el acceso a datos (personales o de otra naturaleza). Esta disposición establece el deber de los PSIL de incorporar en las CGC una descripción sobre el acceso (técnico y contractual) a datos personales o de otro tipo de los empresarios o los profesionales alojados en la plataforma, así como a los datos de los consumidores que se generen al utilizar los servicios de intermediación en línea. En el tratamiento de datos personales, los PSIL están obligados a cumplir las normas para la protección de las personas físicas contenidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), conocido por las siglas RGPD.

Los operadores de las plataformas deben respetar las reglas del RGPD cuando soliciten y traten datos de los consumidores y usuarios que residan en el territorio de la UE, independientemente del domicilio legal de la empresa, en el entendido que sus normas se aplican a las empresas que tienen su sede fuera de la UE y ofrecen bienes o servicios en territorio europeo, como es el caso de Google, Amazon y otras plataformas internacionales[1].

1 El RGPD introduce en su artículo 3.2 una disposición que declara su aplicación a las organizaciones o empresas extranjeras cuando estas ofrezcan productos o servicios a ciudadanos que residen en la UE. De acuerdo con el contenido de este precepto, el RGPD «se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión (…)».

Los datos deben ser tratados de manera lícita, leal y transparente, de modo que garanticen los derechos de transparencia, información, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad y oposición consagrados en el RGPD.

Para cumplir el derecho de transparencia establecido en el RGPD, el artículo 9.2 del Reglamento P2B obliga a los PSIL a indicar en las CGC una descripción sobre el acceso a los datos personales o de otro tipo (o ambos) que proporcionen los usuarios profesionales o los consumidores. La obligación de transparencia incluye el deber de informar si los PSIL tienen acceso a los datos personales que los usuarios (profesionales y consumidores) faciliten para utilizar dichos servicios, indicando la categoría de datos, las condiciones de acceso y de uso de ciertas categorías de datos.

### *3.5. Procedimientos de reclamación y resolución de conflictos*

El Reglamento P2B también se ocupa de regular los diferentes procesos de reclamación y resolución de conflictos derivados de la prestación de los servicios de intermediación en línea. Los artículos 11 y 12 establecen dos procedimientos diferentes, por un lado encontramos el sistema interno de tramitación de reclamaciones, y por el otro, el mecanismo de la mediación, ambos concebidos como procesos previos, opcionales y voluntarios a una demanda judicial.

El artículo 11.1 exige al operador de la plataforma contar con un proceso interno de gestión de reclamos efectivo, fácilmente accesible y gratuito, sin perjuicio de la posibilidad del derecho de las organizaciones, asociaciones representativas u organismos públicos de iniciar procedimientos judiciales ante los tribunales nacionales competentes. Los PSIL deben incluir en las CGC toda la información pertinente sobre el acceso a su sistema interno de tramitación de reclamaciones, así como su funcionamiento.

El artículo 12.1 regula las condiciones mínimas que deben cumplir los procesos de mediación. Los PSIL tienen la obligación de incluir en las CGC a dos o más mediadores que estén dispuestos a colaborar para llegar a un acuerdo con los usuarios profesionales en el caso de que el procedimiento interno de gestión de reclamos no funcione, y así resolver de manera extrajudicial todo litigio entre el proveedor y los usuarios profesionales. Esta norma es minuciosa y detallada, ya que no solo establece el procedimiento de mediación sino que además se ocupa de determinar los requisitos que deben cumplir los mediadores para desempeñarse como tales, incluyendo requerimientos relacionados con sus conocimientos en el área comercial y en el idioma de las condiciones generales que rigen la relación contractual. También establece los requisitos que deben cumplir las personas que ofrezcan sus servicios de mediación desde fuera de la UE, el uso de tecnologías de información en el proceso y la distribución de los costes de la mediación, indicando que los PSIL soportarán una parte razonable de los costes totales de la mediación en cada caso individual.

A efectos de salvaguardar el derecho fundamental de acceso a la justicia, el artículo 12.5 dispone que todo intento de llegar a un acuerdo a través de una mediación para resolver un litigio, se entenderá sin perjuicio del derecho de los

PSIL y de los usuarios profesionales afectados de iniciar un proceso judicial en cualquier momento durante el procedimiento de mediación o antes o después de este.

## 4. El fomento a los sistemas de autorregulación

Para concluir este estudio considero de especial importancia hacer referencia a la disposición incluida en el artículo 17, que fomenta los sistemas de autorregulación en el sector de las plataformas digitales. Esta norma impone a la Comisión Europea el deber de fomentar la elaboración de códigos de conducta por parte de los PSIL y las organizaciones y asociaciones que los representen, junto con los usuarios profesionales, incluidas las micro, pequeñas y medianas empresas y sus organizaciones representativas, con el fin de contribuir a la correcta aplicación del Reglamento P2B.

En la elaboración de estos códigos de conducta se deben tener en cuenta las características específicas de los distintos sectores en que se prestan los servicios de intermediación en línea, así como las características particulares de dichas empresas. También se estimulará la aplicación de los códigos de conducta existentes en el sector. Estos códigos, bien sea que estén elaborados o que en el futuro elaboren los PSIL, los interesados o las organizaciones o asociaciones que los representan, contribuyen a la aplicación correcta del Reglamento P2B, de ahí la importancia de su adopción y uso.

La redacción de los códigos debe contar con una participación de las distintas empresas involucradas en el sector de las plataformas, que son quienes realmente conocen los principales problemas que pueden presentarse en este ámbito. En estos sistemas de autorregulación los PSIL deben tomar en cuenta las consultas con todos los interesados pertinentes, los rasgos específicos de los sectores involucrados, así como las características particulares de las empresas, de manera que su redacción no resulte discriminatoria para ninguno de los sujetos que integran la economía de las plataformas.

## Tres años de vigencia. La evaluación de la Comisión Europea de septiembre de 2023

De acuerdo con el artículo 18 del Reglamento P2B, la efectividad de esta norma debe ser sometida a evaluación por la Comisión Europea cada tres años. Entre los elementos que deben ser evaluados se encuentran el cumplimiento por parte de los PSIL de sus obligaciones relacionadas con la redacción de las CGC y el efecto del Reglamento sobre cualquier desequilibrio en las relaciones entre los PSIL y los usuarios profesionales.

Para cumplir lo previsto en esta norma, el 12 de septiembre de 2023 fue publicado el Informe de la Comisión sobre el primer examen preliminar del Reglamento P2B. Este informe presenta la situación actual del cumplimiento e implementación del reglamento . El informe se basa en encuestas y entrevistas realizadas a los usuarios profesionales de las plataformas y en una evaluación de los términos y condiciones de los contratos de servicios de intermediación

demostrando beneficios tangibles en la aplicación de sus normas. En general el informe refleja efectos positivos en la protección de los empresarios, sin embargo también se observa una falta de cumplimiento por parte de los PSIL y una falta de conciencia de los usuarios empresariales.

## Referencias bibliográficas

Comisión Europea. (2023). *Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the first preliminary review on the implementation of Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services.*

De Miguel Asencio, P. (2019). El Reglamento UE 2019/1150 de servicios de intermediación en línea. En *Pedro de Miguel Asencio* [Blog]. http://pedrodemiguelasensio.blogspot.com/2019/07/reglamento-ue-20191150-sobre-servicios.html

Langlois, R. (2012). Design, Institutions, and the Evolution of Platforms. *Journal of Law, Economics & Policy, 9*(1), 14.

Rico Carrillo, M. (2002). El uso de sistemas de inteligencia artificial y la protección de los empresarios en las plataformas digitales. En L. Cotino Hueso (Dir.) y M. Bauzá Reilly (Coord.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (237-258).

Rodríguez de las Heras, T. (2018). Rules for Electronic Platforms: the Role of Platforms and Intermediaries in the Digital Economy: A Case for Harmonization. *Le droit international privé dans le labyrinth des plateformes digitales*. Institut Suisse de Droit Comparé.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 57-62

# INTELIGENCIA ARTIFICIAL GENERATIVA Y DERECHOS TUTELADOS POR EL DERECHO DE AUTOR

## El caso de New York Times vs. Microsoft Corporation y OpenAI

*GENERATIVE ARTIFICIAL INTELLIGENCE AND COPYRIGHT*

*The case of New York Times vs. Microsoft Corporation and OpenAI*

**Rodrigo Alejandro Gómez Torre**
Universidad de Salamanca

**Eugenia Valeria Grosso**
Universidad Nacional de Cuyo

**María Alejandra Pelegrina**
Universidad Nacional de Cuyo

**Amira Zajur Ramón**
Universidad Nacional de Cuyo

## Resumen

El artículo versa sobre el conflicto jurídico suscitado en el área de los derechos de autor frente a la aparición tecnológica de los LLM y su posibilidad de generar texto a petición del prosumidor. Para circunscribir el tema planteado se hace foco en la actual disputa judicial entre el New York Times y Microsoft Corporation y OpenAI. Este artículo de carácter divulgativo, además de poseer una caracterización de los sujetos y derechos implicados en el pleito, aporta conclusiones sobre la utilidad de este proceso en los sistemas ajenos al *common law*.



## Palabras clave

Inteligencia artificial generativa, derechos de autor.



## Abstract

This paper deals with the legal conflict that has arisen in the area of copyright due to the technological appearance of LLMs and their possibility of generating text at the prosumer's request. In order to circumscribe the issue, the focus is on the legal dispute that the New York Times currently has with Microsoft Corporation and OpenAI. This informative article, in addition to characterizing the subjects and rights involved in the process, provides conclusions on the usefulness of this process in systems outside the common law.



## Keywords

Generative artificial intelligence, copyright.

## Introducción

Frente al auge de los trabajos jurídicos que procuran analizar la inteligencia artificial generativa (en adelante, IAG), quisiéramos comenzar recordando que este fenómeno se sustenta en *algoritmos computacionales* (Aparicio Vaquero, 2022) que incorporan arquitectura de red neuronal, denominada *transformer,* y que en el ámbito científico esta tecnología ya tiene más de un lustro, si se toma como hito la publicación del 12 de junio del 2017, *Attention is all you need, Advances in neural information processing systems* (Vaswani, 2017).

Es cierto que cuando el avance científico irrumpió en el mercado, los algoritmos adquirieron un denominativo más susceptible de publicitar, el de IAG, y con la penetración masiva[1] del fenómeno técnico fue cuando los diferentes sujetos de derecho, que circundan las creaciones autorales, hicieron foco en la porción de mercado que perdían con esta nueva irrupción.

En la actualidad existen diferentes plataformas que utilizan la inteligencia artificial generativa para brindar servicios en forma indiscriminada a los diversos prosumidores que se registran en sus sistemas. Quisiéramos destacar que utilizar la palabra *plataformas* es una licencia lingüística que se ha puesto de moda para identificar a intermediarios o prestadores de servicio de internet, incluso prestadores de servicio contenido en línea (en el lenguaje técnico jurídico del Reglamento (UE) 2022/2065, «Reglamento de Servicios Digitales»)[2].

Este artículo hace foco en la IAG, es decir, aquella que incorpora modelos discriminadores o transformadores (*transformers*) entrenados en un *corpus* o conjunto de datos capaz de mapear la información de entrada en un espacio latente de alta dimensión (Chang *et al.*, 2023). Estos sistemas poseen un modelo generador que impulsa un comportamiento estocástico, creando contenido novedoso en cada intento, incluso con los mismos estímulos de entrada.

Dentro de estos sistemas encontramos una subcategoría de IAG, los llamados modelos de lenguaje de gran escala (o LLM, por su acrónimo en inglés), que se especializan en generar texto.

La aparición de ChatGPT tuvo gran resonancia en la sociedad (y en el mercado), particularmente entre quienes se dedicaban a la explotación (y comercialización) de las creaciones autorales. Los tradicionales sujetos de derechos de autor se han visto interpelados, sobre todo, por la opacidad con que se entrena a estos sistemas. Esta falta de claridad ha llevado a que algunos de estos sujetos acuerden con las empresas titulares de la IAG una contraprestación por la supuesta explotación de sus obras para parametrizar estos algoritmos computacionales.

1 Open IA (y Microsoft Corporation) pusieron en marcha el GPT-1 en 2018, sin embargo, el lanzamiento comercial y masificación acaeció en noviembre del 2022 con el lanzamiento al mercado y los refuerzos publicitarios de ChatGTP. Esta plataforma alcanzó un impresionante poder de penetración, obteniendo 100 millones de usuarios en dos meses. Para que el lector tenga posibilidad de comparar este proceso con el de otras plataformas, Instagram necesitó 26 meses para alcanzar el mismo número de usuarios, Facebook precisó 54 meses y Twitter (ahora X) consumió 65 meses para alcanzar ese nivel de penetración.

2 Sobre el rol y la importancia de estos intermediarios nos hemos pronunciado en Gómez Torre (2023).

En otros casos, cuando el punto de acuerdo no se ha podido conseguir entre los particulares, terminaron por acudir a los tribunales, como lo expondremos en el siguiente apartado.

## Presentación del caso

El 27 de diciembre de 2023, New York Times Company (en adelante, NYT) presentó una demanda en el Distrito Sur de Nueva York en contra de Microsoft Corporation y OpenAI, alegando infracción de derechos de autor (*copyright*) y solicitó que el procedimiento se desarrolle bajo la modalidad de juicio por jurados, en los estrados de un sistema de *common law*.

El demandante aduce que las herramientas de IAG de los demandados, de OpenAI y Bing Chat (o Copilot) de Microsoft[3], contienen y se nutren de una «masa de obras que son de titularidad del New York Times».

NYT afirma que OpenAI y Microsoft infringieron sus derechos subjetivos sobre las obras de las que son titulares al hacer uso y reproducción de estas, sin licencia alguna, durante el entrenamiento de sus modelos.

En primer término, la accionante aporta pruebas periciales a la causa en las que se evidencia que los LLM, eventualmente, «memorizan» parte de los trabajos incluidos en los datos de formación, lo que arroja como resultado que los modelos, en ocasiones, generen reproducciones casi textuales de las obras con las que fueron parametrizados y, como si fuera poco, no se cita la fuente (o el enlace) del contenido, que en el caso en análisis resultan ser los artículos periodísticos producidos por NYT.

En segundo lugar, este proceder ofrece resultados de búsqueda «sintéticos» que reproducen, para el caso de que el *prompt* (instrucción) del prosumidor así lo requiera, «contenido significativamente más expresivo de un artículo original que lo que tradicionalmente se mostraría mediante una búsqueda en línea».

El NYT aduce que el producto ofrecido por las demandadas impacta fuertemente en dos aspectos; tiene una incidencia directa en el ejercicio de la labor periodística y su función en los autodenominados «Estados democráticos»; y además, es una herramienta que permite a los lectores eludir el muro de pago del NYT, lo que se traduce en cuantiosas pérdidas económicas.

Alega también el actor que el conflicto no es meramente una cuestión empresarial de pérdida de ganancias en el marco de un mercado emergente dónde se están vulnerando los derechos consagrados en la *Copyright Act*, sino que, además, y mucho más alarmante, el modelo de negocios de las demandadas pone en jaque la democracia y resulta peligroso para el devenir del conjunto de la sociedad.

El accionante funda sus pretensiones en la Primera Enmienda de la Constitución de los Estados Unidos de 1789, sobre la libertad de expresión y de prensa

3 Desarrollados sobre el modelo GPT de OpenAI, que se basa en modelos de lenguaje de gran escala (LLM) que se construyen mediante «entrenamiento» o parametrización con corpus masivos de textos o datos.

(*right to free speech*, *right to free press*)[4], aduciendo que estos derechos constitucionales sirven para que la prensa esté libre del control gubernamental y así pueda fiscalizar a los gobernantes.

Al mismo tiempo manifiesta que la *Copyright Act* de 1976, en el capítulo 8, sección 107, delimita el *fair use* de las obras[5] y que la utilización de las normas realizada por las demandadas no encuadra en el supuesto.

A su turno, las demandas manifiestan, primeramente, estupefacción por el apartamiento del NYT a un posible acuerdo entre partes; alegan que la tecnología de IAG, como ChatGPT o Copilot, está atrayendo miles de millones de dólares en financiación a la jurisdicción donde discurre el pleito; realiza comparaciones entre los LLM y otras tecnologías previas que irrumpieron frente a los modelos de negocios preestablecidos (se cita como un ejemplo a las videograbadoras).

Su argumento más enérgico es que, para el «entrenamiento» de su tecnología, utilizan una amplia variedad de textos (datos) en línea que van desde artículos periodísticos hasta poemas; pretenden encuadrar en el *fair use* el tratamiento de las obras de autoría de NYT utilizadas, por considerarlas «noticias de dominio público» que, mediante el sistema por ellas desarrollado, intervienen en la creación de material nuevo.

Finalmente, las reclamadas arguyen que resulta absurdo pretender impedir a los modelos de IAG el tratamiento de publicaciones periodísticas, cuando otras organizaciones de noticias no impiden ni pueden impedir que el NYT informe sobre hechos en los que no tuvo ningún papel investigativo.

Las demandas sostienen que a la luz de la *Digital Millennium Copyright Act*, su actividad no implica ninguna vulneración de derechos, sin embargo, otorgar a la demandante la posibilidad de monopolizar hechos periodísticos sí lo es.

## Conclusiones

Se puede apreciar cómo en el caso concreto entran en tensión intereses de dos intermediarios diferentes. Las mutaciones por las que ha pasado a lo largo del tiempo la institución jurídica denominada derechos de autor han llevado a que, frente a un nuevo modelo de negocio, los antiguos intermediarios vean afectados sus intereses.

Estas tensiones van a seguir surtiendo efecto hasta que no se determine en forma cabal el rol de los intermediarios y sus responsabilidades frente a las obras creadas por sus dependientes o prosumidores.

Estimamos que el criterio utilitarista primará, una vez más, para decidir el conflicto de partes y será ese el trasfondo con el que se harán las interpretaciones de la normativa que regula el *fair use*.

4 Se puede consultar la normativa referenciada en el siguiente enlace: https://www.whitehouse.gov/about-the-white-house/our-government/the-constitution/.

5 Se puede consultar la normativa en: https://www.copyright.gov/reports/guide-to-copyright.pdf, así como un análisis de la sección en cuestión en: https://www.copyright.gov/policy/section108/discussion-document.pdf.

Este proceso puede constituirse en un hito debido a la trascendencia de los actores y el contexto (la disputa en un país central). Sin embargo, no será de fácil extrapolación a los sistemas jurídicos con base continental europea, ya que, a pesar de la recepción de la regla de los tres pasos en el Convenio de Berna y en el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, las normas internas de este conjunto de países son más restrictivas en cuanto a la explotación de obras de terceros sin la licencia pertinente otorgada por el titular de la obra.

Estimamos que para estas jurisdicciones (por no individualizarlas como mercados), siempre estará vigente la posibilidad de los acuerdos entre partes, como la forma más habitual de resolución de conflictos frente a la concreción de la amenaza de retirar «la plataforma» de ese determinado país, si es que algún Estado tuviera la intención de aplicar algún tipo de responsabilidad sobre estos intermediarios. Es decir, el criterio utilitarista operando en forma directa en el mercado o en otros órganos que no son estrictamente el órgano judicial.

Por ello consideramos que el desempeño de la Unión Europea como órgano supranacional, atrasado en este tipo de tecnología, pero con un mercado y una posición política y económica preponderante, será de sumo interés para el resto de las jurisdicciones.

## Referencias bibliográficas

Aparicio Vaquero, J. (2022). Derecho de autor y más allá algoritmos, código de los programas de ordenador y apps. *Revista de propiedad intelectual*, (71), 13-98.

Chang, Y. *et al*. (2023). A Survey on Evaluation of Large Language Models. *arXiv. org e-print archive*. https://doi.org/10.48550/ARXIV.2307.03109

Estados Unidos de América. (1789). *Constitución de los Estados Unidos de América de 1789. Primera Enmienda, sobre la libertad de expresión y de prensa*.

Gómez Torre, R. (2023). Plataformas digitales como medios para la concreción de violencia digital en contexto de género. *Informática y Derecho: Revista Iberoamericana de Derecho Informático,* Segunda Época, (13), 149-160

United States Copyright Office. (1977). General Guide to the *Copyright Act of 1976*. https://www.copyright.gov/reports/guide-to-copyright.pdf

Vaswani, A., *et al*. (2017). Attention is all you need, Advances in neural information processing systems. *arXiv.org e-print archive*. https://arxiv.org/abs/1706.03762v7.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 63-69

# LA INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE LOS DERECHOS DE AUTOR: ANÁLISIS SOBRE LA REGULACIÓN EN LA NORMATIVA BOLIVIANA

*ARTIFICIAL INTELLIGENCE AND COPYRIGHT PROTECTION: ANALYSIS OF BOLIVIAN REGULATIONS*

**Andrés Ignacio Blanco Aranibar**
**Juan Carlos Iván Cejas Estrada**

Estudiantes de Derecho y Ciencias Jurídicas,
Universidad Privada del Valle (Bolivia)

## Resumen

El objetivo principal de la investigación es determinar si la normativa de derechos de autor en Bolivia proporciona una protección adecuada frente a los desafíos presentados por el avance de la inteligencia artificial. Se busca evaluar si las leyes actuales son suficientes para salvaguardar los derechos de autor en un contexto donde la inteligencia artificial juega un papel cada vez más significativo en la producción y distribución de contenido.



## Palabras clave

Inteligencia artificial, derechos de autor, creación, protección.



## Abstract

This research analyzes the current legal provisions in Bolivia related to artificial intelligence, with the purpose of determining whether it provides adequate copyright protection in the context of this emerging technology.



## Keywords

Artificial intelligence, copyright, author, creation, protection.

## Introducción

Si bien en Bolivia se encuentra vigente la Ley 1322 de Derecho de Autor y su reglamento, en la actualidad encuentra crítica por parte de algunos sectores por ser obsoleta y no adaptarse a los cambios tecnológicos y sociales de los últimos años, más aún si se considera la aparición de la inteligencia artificial como un programa capaz de generar información a través de la recopilación informática que realiza, siendo un caso de especial atención la protección de los derechos de los creadores e innovadores en la sociedad actual.

Esta investigación analizará en detalle la importancia de la normativa protectora de los derechos de autor y su relación con la inteligencia artificial.

## Marco teórico

### 1. ¿Qué es la inteligencia?

La inteligencia en un sentido literal o semántico se puede entender como la capacidad de entender o comprender, la capacidad de resolver problemas (Real Academia Española, s. f.). Pero no solo se tiene que encerrar la compresión de la palabra «inteligencia» en un sentido semántico, también para un entendimiento más extenso necesariamente se tiene que conocer cómo surge el término, este fue utilizado en un contexto científico por primera vez por Francis Galton, quien en su libro *El genio hereditario*, de 1869, considera a la inteligencia como una capacidad física y que sería heredada (Maureira Cid, 2017, p. 19).

### 2. ¿Qué es la inteligencia artificial?

Desarrollado el concepto de «inteligencia», el concepto de «inteligencia artificial» es más asequible de discernir. La IA puede ser entendida como la ciencia e ingeniería que permite diseñar y programar ordenadores de forma que realicen tareas que requieren inteligencia (Meseguer González y López de Mántaras Badia, 2017).

Esta recopila información para un posterior procesamiento de la misma, siendo el resultado de tratamiento de datos, que tienen como fin dar respuesta de la petición solicitada por el usuario, no siendo un proceso intelectual el efectuado por la IA.

### 3. ¿Qué se entiende por «autor»?

Para la comprensión de este término la presente investigación se basará en el glosario de términos de la OMPI, publicado en Ginebra, Suiza en 1980, que da el siguiente concepto: «es la persona que crea una obra» (p. 25), resaltando la palabra «persona».

### 4. ¿Qué son los derechos de autor?

Para definir qué son los derechos de autor, esta investigación utilizará la interpretación que emana del Tribunal Federal de Brasil, el cual considera que «el derecho de autor no es sino una extensión, una ampliación, una exteriorización del derecho de propiedad» (Antequera Parilli, 2007).

## Marco jurídico

### 1. Constitución Política del Estado Plurinacional de Bolivia

La norma suprema del ordenamiento jurídico boliviano asegura la protección integral de los derechos de propiedad intelectual, tanto a nivel individual como colectivo, en beneficio de los autores, compositores o artistas (art. 102). En ese sentido, y con el respaldo del art. 410 de la ley fundamental, se establece la aplicabilidad de tratados internacionales como parte del bloque de constitucionalidad[1], fortaleciendo así la protección de los derechos a nivel nacional e internacional.

### 2. Ley 1322 del 13 abril de 1992 (Ley de Derecho de Autor)

Es pertinente resaltar que la normativa específica aplicable a los derechos de autor tiene una antigüedad considerable en Bolivia. Sin embargo, su contenido *prima facie* suele ser suficiente para cumplir con la finalidad protectora del derecho de autor.

En ese contexto, resulta fundamental resaltar el reconocimiento que la ley otorga a los derechos de autor, los cuales comprenden tanto a los derechos morales, como a los patrimoniales (art. 1, Ley 1322). Bajo esa lógica, la normativa considera que la protección del derecho de autor se extiende a toda creación literaria, artística, científica, cualquiera sea la forma de expresión y el medio o soporte tangible o intangible actualmente conocido o que se conozca en el futuro (art. 6, Ley 1322).

En cuanto a la titularidad del derecho la normativa hace una diferenciación entre quienes pueden ser considerados autores y quienes pueden ejercer los derechos de autor sobre una obra. Respecto al primer punto se considera titular únicamente a la persona natural y sobre el ejercicio de los derechos el legislador entiende que las personas jurídicas (Estado, empresas u otros) son titulares derivados aunque no hayan creado una obra personalmente.

1 Artículo 410, parágrafo II de la Constitución Política del Estado: «La Constitución es la norma suprema del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa. El bloque de constitucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas de Derecho Comunitario, ratificados por el país».

## 3. Decisión 351 de la CAN (Régimen Común sobre Derecho de Autor y Derechos Conexos)

La Comunidad Andina, antiguamente conocida como Pacto Andino, es un proceso de integración que ha estado en marcha en América Latina desde 1969 con la firma del Acuerdo de Cartagena. Este acuerdo fue suscrito por Bolivia, Colombia, Chile, Ecuador, Perú y, posteriormente, Venezuela. Tuvo como objetivo armonizar los derechos de autor en la región andina, garantizando la adecuada y efectiva protección a los autores y titulares de derechos sobre las obras de ingenio en los ámbitos literario, artístico o científico, independientemente de su género o forma de expresión.

A los fines antes mencionados se considera como autor a toda persona física que realiza creación intelectual (art. 3, Decisión 351), siendo este el titular de los derechos morales y patrimoniales que comprende el mismo, sin perjuicio de que un tercero como personas morales o jurídicas pueda ostentar los derechos derivados de la creación intelectual.

## 4. Servicio Nacional de Propiedad Intelectual (SENAPI)

A través del Decreto Supremo n.º 27.938 se crea el SENAPI, una institución pública desconcentrada, con competencia de alcance nacional, dependiente del Ministerio de Desarrollo Económico y con dependencia funcional del viceministro de Industria, Comercio y Exportaciones (art. 2).

El SENAPI administra en forma desconcentrada e integral el régimen de la propiedad intelectual en todos sus componentes, constituyéndose en la oficina nacional competente respecto a los tratados internacionales y acuerdos regionales suscritos y adheridos por el país (art. 4). Su régimen se basa en las normas bolivianas y los convenios internacionales, además de las normas comunitarias en materia de propiedad intelectual.

Bajo un análisis de este decreto supremo se puede lograr comprender que, aunque la normativa boliviana aún no es suficiente para proteger los derechos de autor frente a las nuevas tecnologías que aparecen apresuradamente en el mundo, esta encuentra su solución en la vía internacional, debido a que permite y exige la aplicación de los tratados internacionales dentro de la institución.

## 5. Organización Mundial de Propiedad Intelectual (OMPI)

Desde la adhesión de Bolivia a la OMPI en 1993, el Estado suscribió cinco convenios, entre los cuales se encuentran el de «Derecho de Autor». Lo más relevante de este tratado para la presente investigación recae en los arts. 2 (ámbito de la protección del derecho de autor), 4 (programas de ordenador) y 5 (compilaciones de datos). Con el art. 2 se entiende que para que exista el derecho de autor necesariamente tiene que estar expresada materialmente[2]. Respectivamente, el

2 Artículo 2 del Tratado de Derechos de Autor de 1996: «La protección del derecho de autor abarcará las expresiones pero no las ideas, procedimientos, métodos de operación o conceptos matemáticos en sí».

art. 4 establece que los programas de ordenador están protegidos como obras literarias, cualquiera que sea su modo o forma de expresión[3]. El art. 5 regula que la compilación de base de datos, en cualquier forma, por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, está protegida como tal, especificando que la protección no abarca los datos en sí mismos y se entiende sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales contenidos en la compilación[4].

Al analizar estos tres artículos se puede entender que:

1) La IA, al ser un programa de ordenador que se encarga de la recopilación de datos para un posterior procesamiento que plasma una representación solicitada, esto bajo el modelo de procesamiento simbólico (Aguilera García, 2007), no puede considerarse como una creación humana.
2) Las obras creadas con IA tendrían como legítimo autor del derecho a los autores intelectuales de los datos recopilados, según el análisis de los artículos ya mencionados del tratado de derechos de autor.

## Metodología

Los métodos empleados en la presente investigación fueron: deductivo, por cuanto se analizó de forma general la normativa hasta el enfoque particular de esta; inductivo, que tuvo como objetivo encontrar normativa específica; jurídico, debido al análisis de la legislación boliviana; exegético, por cuanto se analizó específicamente los artículos pertinentes al derecho de autor; y semántico, debido a la contextualización de ciertas definiciones necesarias para entender y relacionar con la investigación.

## Análisis y consideraciones

Entonces, dado que la información generada por la inteligencia artificial no es el resultado de la actividad humana directa, no puede considerarse como producto de un autor humano. La IA sigue instrucciones y su resultado puede ser incierto, lo que contrasta con el proceso creativo consciente y deliberado de un autor humano. Para ser considerado autor, uno debe aplicar su originalidad conscientemente, convirtiéndose en creador de una obra. En este sentido, la cotitularidad no sería apropiada, ya que no se puede fusionar un contenido generado por IA con la creación humana. Es necesario separar estas contribuciones, ya

3 Artículo 4 del Tratado de Derechos de Autor de 1996: «Los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión».

4 Artículo 5 del Tratado de Derechos de Autor de 1996: «Las compilaciones de datos o de otros materiales, en cualquier forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, están protegidas como tales. Esa protección no abarca los datos o materiales en sí mismos y se entiende sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales contenidos en la compilación».

que esto afectará el proceso de registro en el SENAPI. Además, la inteligencia artificial no puede ser considerada autora de una obra derivada, ya que carece de conocimiento sobre la obra original que deriva de ella

## Conclusiones

En conclusión, en el contexto jurídico de Bolivia la normativa dispone que únicamente las personas naturales pueden ser reconocidas como autoras, excluyendo así la posibilidad de atribuir autoría a la inteligencia artificial, debido a que esta es una facultad inherente a la capacidad de creación intelectiva humana. Esto debido al carácter personalísimo, irrenunciable e imprescriptible del derecho de autor, destacando la importancia de proteger la relación directa entre el creador humano y su obra.

## Referencias bibliográficas

Aguilera García, E. R. (2007). *Inteligencia artificial aplicada al derecho*. Instituto de Investigaciones Jurídicas, UNAM.

Antequera Parilli, R. (2007). *Estudios de derecho de autor y derechos afine*s. Reus.

Bolivia. (1992). Ley 1322. Ley de Derecho de Autor. *Gaceta Oficial del Estado Plurinacional de Bolivia*.

Bolivia. (1997). *Decreto Supremo 27.938*.

Bolivia. (2009). Constitución Política del Estado Plurinacional de Bolivia.

Comunidad Andina de Naciones. (1993). *Decisión 351. Régimen Común sobre Derecho de Autor y Derechos Conexos*.

Maureira Cid, F. (2018). *¿Qué es la inteligencia?* Bubok Publishing.

Meseguer González, P., López de Mántaras Badia, R. (2017). *Inteligencia artificial*. Consejo Superior de Investigaciones Científicas.

Organización Mundial de la Propiedad Intelectual. (1980). *Glosario de Términos de la Organización Mundial de la Propiedad Intelectual*.

Organización Mundial de la Propiedad Intelectual. (1996). *Tratado de Derechos de Autor*.

Real Academia Española. (s. f.). Inteligencia. *Diccionario de la lengua española* (23.ª ed.). https://dle.rae.es.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 71-78

# DESAFÍOS Y OPORTUNIDADES EN LA GOBERNANZA DEL INTERNET EN LA ERA DE LA CONVERGENCIA TECNOLÓGICA

*CHALLENGES AND OPPORTUNITIES IN INTERNET GOVERNANCE IN THE ERA OF TECHNOLOGICAL CONVERGENCE*

**Nicole Angel Sánchez Rojas**

Federación Iberoamericana de Asociaciones de Derecho e Informática

## Resumen

El artículo realiza un análisis de la innovación desde la perspectiva de la convergencia tecnológica, explicando que para poder discutir y analizar las tecnologías disruptivas, es necesario entender la infraestructura requerida para su funcionamiento, es decir, el internet. Además, el artículo examina las brechas de conectividad e innovación tecnológica existentes en América Latina, demostrando cómo estas brechas pueden influir en la economía de uno o varios países. Por lo tanto, plantea la cuestión de si antes de hablar de regulaciones sobre inteligencia artificial, deberíamos mejorar la infraestructura y gobernanza del internet.



## Palabras clave

Convergencia tecnológica, gobernanza del internet, brechas de conectividad, tecnologías disruptivas, infraestructura del internet.



## Abstract

This paper analyzes innovation from the perspective of technological convergence. It explains that in order to discuss and analyze disruptive technologies, we must understand the infrastructure required for their operation, namely the internet. Additionally, the article examines the connectivity and technological innovation gaps that exist in Latin America, demonstrating how these gaps can influence the economy of one or several countries. Consequently, it raises the question of whether we should improve internet governance and infrastructure before discussing regulations on artificial intelligence.



## Keywords

Technological convergence, internet governance, connectivity gaps, disruptive technologies, internet infrastructure.

## Introducción

Internet no es una red única, aunque su funcionamiento así lo parezca, es una red de redes que coordinan entre sí en todo el mundo. Para entender el funcionamiento de innovación, internet, convergencia tecnológica o tecnologías disruptivas, se debe tomar diferentes factores, como la infraestructura que existe por detrás, y el impacto que puede tener en la sociedad.

Antes de analizar qué son las tecnologías disruptivas (*big data*, IOT, inteligencia artificial, etc.) debemos hacer referencia a la infraestructura que sostiene esto, el internet, que está compuesto por puntos de intercambio de tráfico (PIT), proveedores de servicios de internet (ISP), protocolos de internet (IP), sistemas de nombres de dominio (DNS), entre otros, regulados a través de múltiples *stakeholders* a nivel nacional, regional y global.

Con la implementación de tecnologías, específicamente computadores e internet, el mundo mostró un ritmo de cambio superior al observado anteriormente, la automatización de procesos fue la fuente de muchas innovaciones y cambios a nivel mundial.

Tras las nuevas innovaciones se comienza a mencionar de nuevas normativas y reglamentos, como la Unión Europea y la norma sobre inteligencia artificial, sin embargo, debemos recordar que la base del funcionamiento de todas estas innovaciones tecnológicas es el internet, por lo cual también se debe pensar en una actualización dentro de la gobernanza del internet. Al encontrarnos en la era de la sociedad de la información y sociedad del conocimiento hay muchos puntos que debemos tomar en cuenta, el nivel de accesibilidad a estas nuevas tecnologías, el impacto en la sociedad y la salvaguarda de los derechos de las y los ciudadanos.

## Desarrollo del internet y su importancia en el desarrollo de tecnologías disruptivas

En 2024 se cumplen 55 años desde el primer mensaje enviado a través de internet, dentro de este período de tiempo se observó una evolución a nivel internacional en temas de gobernanza del internet a través de organizamos internacionales, siendo el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC) (Aguerre, 2019) quien regula estos temas a nivel latinoamericano y abarcando parte del Caribe. Dentro de esta evolución se observó la creación de reglas para el funcionamiento del internet, así como un ecosistema para su funcionamiento e identificación de redes.

Para entender la necesidad de realizar actualizaciones en la gobernanza del internet, así como los retos que trae consigo la convergencia tecnológica y el avance de las tecnologías disruptivas, es necesario que entendamos como funciona la infraestructura del internet. Por lo cual de manera breve observaremos algunos de sus componentes.

## 1. ISP

Dentro del funcionamiento del internet, las empresas proveedoras de internet (ISP, por las siglas en inglés de *Internet Service Providers*) tienen un rol fundamental para la gestión de las diferentes redes. Estos proveedores de acceso a internet se interconectan a través de infraestructuras que cuentan con un protocolo (TCP/IP, por las siglas en inglés de *Transmission Control Protocol/ Internet Protocol*). Son protocolos de control de transmisión o protocolos de internet, se usan en internet para que los ordenadores y otros dispositivos envíen y reciban datos, y funcionan en cualquier tipo de infraestructura, adaptándose de una manera adecuada.

## 2. Punto de intercambio de tráfico

Los puntos de intercambio de tráfico (PIT) son infraestructuras críticas que permiten que diferentes redes intercambien tráfico de internet de manera local y eficiente, reduciendo la dependencia de proveedores de tráfico internacional, lo que puede mejorar significativamente la calidad y costo del servicio de internet.

> Los Puntos de Intercambio de Tráfico (PIT) son ubicaciones físicas estratégicas donde se instalan servidores que facilitan la conexión entre diferentes redes de internet. Estos puntos permiten a los proveedores de servicios de internet y a las redes intercambiar datos de manera más eficiente y económica al comprar capacidad de conexión de forma conjunta. La presencia de PIT en un país es un indicador de la madurez de su infraestructura de internet. (Cavalli, 2018).

La expansión y fortalecimiento de los PIT en América Latina es esencial para mejorar la conectividad dentro de la región y disminuir los costos asociados al acceso a internet. A diferencia de lo que se cree, la conectividad al internet se da a través de cables submarinos (*landing points*) en su mayoría, y no a través de satélites, siendo estos la fuente mínima de conectividad y para contenido determinado, como multimedia con un gran ancho de banda (Internet Society, 2014).

## 3. IP y DNS

Dentro del funcionamiento de la infraestructura del internet se debe mencionar también la asignación de protocolos de internet (IP) y nombres de dominio (DNS). Si bien cada sitio web cuenta con un IP, nosotros solemos conocerlos a través de un nombre de dominio, ya que es más fácil de recordar que un código o IP, que es un conjunto de números que identifican a las redes de internet, una identificación única que tiene cada cosa, persona, servidor, red o dispositivo. Dentro de esto hay dos términos que debemos mencionar: son los *IPv4* y los *IPv6*, que se definen así por las versiones y el número de cifras que tienen sus códigos. En la evolución de la infraestructura de internet,

> la asignación de direcciones IP y nombres de dominio ha tenido que expandirse para acomodar el crecimiento exponencial de dispositivos y servicios en línea. La implementación de IPv6 y la gestión eficiente de los nombres de

> dominio son cruciales para mantener la funcionalidad y seguridad de la internet. (Cavalli, 2018).

Estas direcciones IP son gestionadas por diferentes organizaciones según la región en la que nos encontremos. Las direcciones IP se reparten a través de organizaciones, denominadas *Regional Internet Registries*, o registros regionales de internet, dentro de estas organizaciones se tiene a: ARIN, Norteamérica y parte del Caribe; LACNIC, América Latina y parte del Caribe; RIPE, NCC, Europa y Asia; APNIC, Australia; AFRINIC, África.

## La convergencia tecnológica

Tras haber analizado los anteriores puntos que son parte fundamental de la infraestructura del internet, podemos hablar sobre convergencia tecnológica, que es la integración de tecnologías separadas en sistemas que trabajan de forma colaborativa, involucrando tecnologías clave como la inteligencia artificial, el *big data*, la internet de las cosas (IOT), entre otras.

> La mayoría de las nuevas tecnologías cuando aparecen, normalmente ganan, de inmediato, el título de «el próximo gran cambio», pero la mayoría no genera este impacto porque no cuenta con las características esenciales de escalabilidad, costo e impacto en la sociedad en conjunto. (Scartezini, 2018).

¿Pero por qué debemos entender sobre la infraestructura del internet antes de hablar de convergencia tecnológica? La convergencia tecnológica dio lugar a que las personas puedan acceder a una mayor cantidad de servicios, ya sea de comunicación, trabajo, educación, redes sociales, de investigación o de entretenimiento, sin embargo, lo que para muchos es un beneficio, para otros puede ser un obstáculo relacionado a la brecha digital y la brecha de conexión a internet.

Por lo tanto, observamos que uno de los mayores obstáculos para esta convergencia tecnológica es la brecha de conectividad a internet, lo que muestra la necesidad de actualizar los marcos normativos que conocíamos dentro de lo que es la gobernanza del internet,

> para alcanzar los objetivos mencionados y generar un entorno apto para la implementación de los servicios de telecomunicaciones y TIC, se requiere en forma indispensable una adecuada infraestructura de telecomunicaciones y es por ello que las políticas públicas tienen su foco en el despliegue de infraestructura. (Belli, 2018).

## Retos en América Latina frente a la convergencia tecnológica

La convergencia tecnológica ha transformado el acceso y la funcionalidad del internet, colocando a América Latina ante desafíos únicos y oportunidades sin precedentes en la gobernanza del internet, con el desarrollo de tecnologías emergentes como el *big data*, IOT o la inteligencia artificial, que están redefiniendo las políticas de regulación y la administración de los recursos tecnológicos en la región. El internet tuvo y tiene un gran impacto en el desarrollo de la economía a nivel global, lo cual nos lleva a un punto importante, las empresas con mayor

crecimiento económico en el ámbito tecnológico se encuentran en Estados Unidos y China, mientras que América Latina es consumidor de este tipo de servicios. En un mundo donde la conectividad a internet es un vector importante en el crecimiento económico, los países con brechas en el acceso al internet llegan a ser los perjudicados, quedando pasos atrás de los países con mayores recursos de conectividad. De 8000 millones de personas que habitan el mundo, solamente 5.35 billones de personas utiliza internet, por lo cual se quedan al margen de hechos y conocimiento que existen en el mundo, teniendo como un aproximado de 2.7 billones de personas que no tienen acceso a internet (Unión Internacional de Telecomunicaciones, 2022).

Si mencionamos que el internet llega a ser una herramienta y que la convergencia tecnológica nos da acceso a más servicios, también debemos pensar en las limitaciones que da esto a personas que no se encuentran dentro del grupo con acceso a internet o que su acceso es parcial, como ocurre en varias zonas en diferentes países de Latinoamérica, personas de áreas rurales, por ejemplo, y, por último y no menos importante, las brechas de género, tomando en cuenta que por temas de trabajo y responsabilidades en áreas rurales, las mujeres tienen aún menor oportunidad de acceso a internet.

Las diferencias sociales, de inclusión económica y social, así como las brechas de género continúan siendo temas no resueltos por la humanidad, tanto que

> en el establecimiento de los ODS, la humanidad todavía ronda con los mismos problemas de varias décadas, tales como, promoción del crecimiento económico inclusivo; promoción y defensa de los derechos humanos; prevención de conflictos y mantenimiento de la paz entre los pueblos (…) cuando nos posicionamos y analizamos nuestra época bajo la óptica de las telecomunicaciones TIC, existe una alteración sustancial (…). (Ramos, 2018),

Ello nos deja analizando si quizás las medidas que se toman deben cambiar y si el terminar con brechas de conectividad es la base para avanzar en el cumplimiento de los ODS.

## ¿Cómo definir la gobernanza del internet?

Dentro del grupo de trabajo para la gobernanza del internet (WGIG), en 2005 se plantearon los siguientes puntos para definir la gobernanza del internet, haciendo mención a que su desarrollo y aplicación es un trabajo conjunto entre los gobiernos, el sector privado, la sociedad civil, mencionando un trabajo que debe ser multiparticipativo, con la actuación de diferentes *stakeholders*, tomando en cuenta diferentes puntos de vista, dentro de los cuales se debe desarrollar principios, normas, reglas y procedimientos para la toma de decisiones comunes para la evolución y uso del internet (Internet Society, s.f.).

De la misma forma en la que buscamos el desarrollo tecnológico, debemos establecer medidas para la protección de datos, privacidad, intimidad y libertad de las personas, ya no solo en un ámbito físico, sino también en la red. Es así que se observa la evolución de este último derecho y la transversalidad con los dos anteriores, ya que la libertad y la privacidad en un entorno físico resultan ser

derechos más separados, pero en internet la posibilidad de decir algo de manera libre preservando la privacidad es posible y aplicado.

> Bajo la garantía de la «libertad de expresión» universalmente se comprenden la libertad de emitir opinión y el derecho de dar o recibir informaciones o ideas, sin censura previa o sin injerencia de autoridades. Se la considera como una de las garantías fundamentales de las sociedades democráticas, y cualquier persona puede reivindicar que se le respete el ejercicio de esta garantía (…). (Molina, 2018).

## Conclusiones

Se debe mencionar que pensar en regulaciones y gobernanzas no busca limitar el desarrollo tecnológico, sino mas bien establecer lineamientos de desarrollo ético y respetando los derechos de las y los ciudadanos. Tenemos la obligación de informar a la sociedad sobre las diferentes tecnologías y que no todo lo que vemos es inteligencia artificial, concientizando sobre la necesidad de actualizar otras normativas y regulaciones como el tema de la gobernanza del internet.

Antes de pensar en regulaciones de inteligencia artificial los países deben pensar en mejorar el funcionamiento de infraestructura del internet, así como una actualización en su sistema de gobernanza, complementando con actualizaciones en normativas, como la de protección de datos, ya que, con la evolución de los derechos, la privacidad, intimidad y libertad de expresión, son esenciales dentro de la red. Con la actualización de estas normas sería posible contar con lineamientos para el desarrollo de tecnologías 5G, la aplicación de manera ética del *big data*, así como el desarrollo de IA y una adecuada aplicación de la seguridad cibernética. La tecnología e innovación marcan el desarrollo económico mundial, y para buscar que América Latina sea parte de esto, debemos repensar cómo estamos manejando los temas de conectividad y gobernanza del internet, trabajar desde cada país en las brechas de conectividad y trabajar de manera constante en la alfabetización tecnológica, de la mano de políticas públicas adecuadas. Ello ayudaría a cada Estado a cumplir con ciertos objetivos de desarrollo sostenible, como innovación, acceso a la justicia, equidad de género, educación, entre otros.

Un reto seria pues llevar a cabo la actualización de normas para tecnologías emergentes. La rápida adopción de tecnologías como 5G y las aplicaciones de *big data* hacen imperativa la actualización de las normativas para abordar adecuadamente la protección de datos personales y la seguridad cibernética. América Latina debe acelerar el desarrollo de un marco regulatorio que equilibre la protección del consumidor con el fomento a la innovación.

## Referencias bibliográficas

Aguerre, C. (2019). *El desarrollo de la Comunidad de LACNIC*. ICANN. LACNIC. Internet Society. LACTLD. https://www.lacnic.net/innovaportal/file/3733/1/el-desarrollo-de-la-comunidad-de-lacnic.pdf.

Belli, L. (2018). Gobernanza y regulaciones de internet: una presentación crítica. En L. Belli y O. Cavalli (Coords.), *Gobernanza y regulaciones de internet en América Latina* (43-70).

Cavalli, O. (2018). *La gobernanza del internet, su evolución y estado actual*. Consejo Argentino para las Relaciones Internacionales.

Internet Society. (2014). *The Internet Exchange Point. Toolkit & Best Practices Guide*. https://www.internetsociety.org/wp-content/uploads/2021/04/Global-IXPToolkit_Collaborative-Draft_Feb-24.pdf.

Internet Society. (s. f.). *Gobernanza de Internet*. https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetGovernance-20151030-es.pdf.

Molina, E. Privacidad, datos personales y tensiones con la libertad de expresión online. En L. Belli y O. Cavalli (Coords.), *Gobernanza y regulaciones de internet en América Latina* (307-325).

Ramos, B. Las telecomunicaciones invisibles: inclusión y desarrollo social por medios de las telecomunicaciones/TIC. En L. Belli y O. Cavalli (Coords.), *Gobernanza y regulaciones de internet en América Latina* (73-82).

Scartezini, V. Tecnologías disruptivas y sus impactos en América Latina. En L. Belli y O. Cavalli (Coords.), *Gobernanza y regulaciones de internet en América Latina* (437-448).

Unión Internacional de Telecomunicaciones. (2022). *Informe sobre la conectividad mundial de 2022*. https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-GLOBAL.01-2022-SUM-PDF-S.pdf.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 79-85

# DAÑOS COLATERALES DE LA BRECHA DIGITAL Y RELACIÓN CON LA CIBERSEGURIDAD

*COLLATERAL DAMAGES OF THE DIGITAL GAP AND ITS CONNECTION TO CYBERSECURITY*

**Carlos Ramírez Castañeda**

Doctor en Administración y Políticas Públicas (Universidad Anáhuac)

## Resumen

Es innegable el hecho de que nos encontramos viviendo en una sociedad donde internet y las tecnologías se han vuelto indispensables para la realización de diversas labores cotidianas. Los beneficios que apareja el uso tecnológico son varios, desde un desarrollo, impulso, crecimiento y mayores oportunidades. Sin embargo, existe un problema muchas veces desconocido, la brecha digital. Existen poblaciones que no tiene acceso a internet y a las TIC, estas mismas pueden tener consecuencias muchas veces irreversibles, pues, no solamente estamos hablando de un aislamiento, sino también de daños producidos a su integridad en diversos sentidos. Analizamos dos vertientes principales: la primera, consecuencias producidas por la brecha digital a nivel salud, y la segunda, las afectaciones a nivel de ciberseguridad de las que pueden ser parte estas poblaciones. La finalidad de este artículo es lograr un factor de concientización para el lector final.



## Palabras clave

Brecha digital, ciberseguridad.



## Abstract

It is an undeniable fact that we find ourselves living in a society where internet and technology have become essential for carrying out daily tasks. The benefits that come with technology are numerous, such as development, growth and greater opportunities. However, there is a frequently unknown problem — the digital gap. There are populations that do not have access to the internet and ICT, this can often have irreversible consequences, not only in terms of isolation, but also in terms of damage caused to their integrity in many ways. This paper analyzes two main aspects. The first are the consequences produced by the digital gap at the health level. The second, the cybersecurity dangers that these populations may be victims of.



## Keywords

Digital gap, cybersecurity.

## Introducción

México enfrenta un problema (entre muchos otros) invisible a la percepción de las multitudes, un problema que permea a distintas escalas y sus consecuencias pueden verse materializadas a pesar de que se gesta de manera no tangible, en lo digital.

La brecha digital es un tema del que poco se ha hablado y durante el aislamiento pandémico por SARS-CoV-2 se pudo vislumbrar con el alejamiento de la tecnología y habilidades básicas para el manejo de esta, lo cual resultó en un punto de afectaciones a la ciberseguridad e integridad de diversas personas.

¿Por qué lo anterior puede representar un problema que requiere mayor atención? A nivel de ciberseguridad, una persona sin conocimiento preventivo hace que se convierta en un potencial blanco para la ciberdelincuencia, de aquí derivan diversos temas como fraudes, estafas, suplantación, usurpación de identidad, siendo algunos de los daños más comunes.

Todo lo gestado en el ciberespacio y a través de las TIC parecería que no tiene una trascendencia mayor, este paradigma debemos romperlo de inmediato. Aquí es donde nos comenzamos a percatar de los primeros daños que produce la brecha digital, no solamente a nivel de afectaciones digitales, sino también con daños colaterales que pudieran reflejarse en la salud de las poblaciones aisladas, en este caso por lejanía, aislamiento, carencia de recursos y habilidades que los hacen quedar en el olvido y sin mayores oportunidades de crecimiento, desarrollo e incluso interacción.

A pesar de tener una mayoría poblacional con acceso a internet en nuestro país (algo que resulta irónico), las poblaciones más desprotegidas son las que siguen padeciendo de una brecha digital, no solamente poblaciones alejadas que se encuentran en zonas rurales, sino también en partes citadinas donde es complicado el acceso a la tecnología.

Analizamos dos vertientes principales: la primera, las consecuencias producidas por la brecha digital a nivel de salud; y la segunda, las afectaciones a nivel ciberseguridad de las que pueden ser parte estas poblaciones.

El conocimiento preventivo con el análisis mostrado permitirá al lector tener un parámetro preventivo y de concientización.

La brecha digital es un problema latente, no solamente en México, sino en diversos países.

## Desarrollo

Al hablar de tecnología en México, tenemos que analizar diversas aristas, en este caso abrimos con el tema relacionado al acceso a internet, pues se ha convertido en la principal herramienta de acercamiento, conectividad, uso y necesidad para el desarrollo de habilidades básicas al hablar de brecha digital. Sin internet no es posible tener un desarrollo tecnológico en diversas vertientes. Sin un acceso a internet existe una incomunicación que cesa oportunidades de crecimiento, aprendizaje y desarrollo para las personas.

Debemos hacer especial énfasis en cuanto a cifras actuales, pues nos interesa únicamente analizar el contexto reciente de brecha digital, por ello mencionamos al decimonoveno estudio de Usuarios de Internet en México, donde se nos indica que, con corte al 2023, México tiene un 80,8% de población con acceso a internet en todo el país (Asociación Mexicana de Internet, 2023).

Se habla de usuarios conectados, pero se ha dejado a la deriva a usuarios que no tienen la forma incluso de poder obtener un acceso a internet. Como lo mencionábamos al inicio de este artículo, existen aún poblaciones que se han convertido en las olvidadas digitalmente, las cuales resultan vulnerables en materia de ciberseguridad, convirtiéndose en algunos de los principales blancos para la ciberdelincuencia. Las barreras que se encuentran presentes como factores económicos, políticos, sociales, e incluso culturales se pueden ver reflejados en la forma cómo se adopta e integra la tecnología a la vida de esas poblaciones.

Si en algo se relacionan los hogares rurales y urbanos al hablar de internet, es que, uno de los principales factores limitantes para la conectividad es el costo de los servicios, esto lo constata Domínguez (2020) en su publicación al momento de estar razonando sobre la desigualdad digital en México, brindando con ello un análisis de las posibles causas relacionadas al nulo acceso a internet y también a las TIC, principalmente haciendo un hincapié en la parte económica.

Sin duda un primer factor de aislamiento es el económico, en este caso y a pesar de algunas estandarizaciones de tarifa sobre el espectro de uso en los hogares de internet en México, existen otras necesidades a cubrir previamente por las familias, dejando a la tecnología y conectividad en el olvido, por ejemplo, es más importante cubrir una primera necesidad como lo son los alimentos, dejando de lado a las TIC en la lista de gastos.

La brecha digital tiene consecuencias en la salud mental, provoca sentimientos de aislamiento producidos por el entorno social y especialmente un margen de exposición a diversos riegos digitales. Cuando mencionamos que una persona no tiene acceso a internet, debemos preocuparnos.

Los daños colaterales se pueden matizar al desencadenar o exacerbar problemas como ansiedad, insomnio, trauma, paranoia, abuso de sustancias o incluso conductas y acciones suicidas, (Inkster, Knibbs y Bada, 2023). Bajo este análisis estamos ante un escenario que requiere atención, pues la línea entre lo digital y lo físico desaparece para traer consecuencias muchas veces irreversibles.

Si nos adentramos más podemos mencionar a las limitaciones en el acceso a plataformas que pueden ofrecer servicios, contenidos, noticias, dejando en el aislamiento social al no tener un medio para mantenerse en comunicación y conexión con su círculo cercano.

La autoeficacia, o la creencia en la capacidad propia para manejar situaciones y desafíos, puede verse afectada negativamente por la falta de acceso a la tecnología. La incapacidad de usar herramientas digitales que facilitan la vida cotidiana puede disminuir la confianza en las propias habilidades, aumentando la ansiedad y el estrés.

Basta con recordar a los tiempos en donde la educación durante pandemia tuvo que tomar un rumbo a la distancia, educación a través de tecnologías e internet. En el periodo pandémico la deserción escolar fue notoria en diversos sectores educativos, dejando sin capacidad de poder continuar en su formación académica a niños, niñas, adolescentes e incluso adultos por las carencias de acceso a las TIC. Muchos mexicanos seguramente conocemos a alguien que pasó por una situación similar.

La carencia de acceso a internet y las TIC puede limitar las oportunidades, no solamente educativas, si no de desarrollo profesional, con los sentimientos de frustración, baja autoestima y ansiedad, con esto la salud mental se ve afectada.

Hoy en día las TIC y las redes sociales se han convertido en una parte integral de la vida de muchas personas, teniendo una clara influencia cultural, de comunicación y de esparcimiento de información. Sin embargo, las personas que no tienen acceso pueden mostrar sentimientos de exclusión y desconexión de la sociedad, trayendo consecuencias en su identidad y su bienestar emocional.

Ahora bien, ya que lo mencionamos desde una perspectiva un tanto más social, psicológica y relacionada a la salud intrínseca de cada persona como usuario, llevemos este escenario hacia un análisis bajo la óptica de la ciberseguridad.

Una persona sin acceso a las TIC y a internet se puede convertir en un blanco fácil para ser víctima de la ciberdelincuencia, esto con un ejemplo de un ciberataque y técnica de inducción al engaño para hacerse de información privilegiada de la víctima.

El *phishing* es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (INCIBE, s. f.-a). Esta técnica resulta ser «básica» de detectar para personas que están relacionadas con el uso tecnológico, al momento de poder tener una clara identificación y diferenciar entre un sitio o correo electrónico real de uno apócrifo, lo cual alguien parte de la estadística de brecha digital no podría hacer y he ahí el problema matizado, victimas cayendo en el engaño por razones de desconocimiento.

La ciberseguridad requiere importancia, atención y sobre todo interés de la población, pero esto solamente se podría lograr a través de un acercamiento social para los usuarios. El sentido común digital se hace parte de los hábitos de las personas que día a día utilizan tecnología, poco a poco el usuario de manera práctica se va dando cuenta de cómo diferenciar un sitio de *phishing* de uno real.

Cabe aclarar que no podemos hablar de cifras exactas relacionadas a problemas de ciberseguridad en México, pues vivimos ante un escenario de carencia de cultura sobre la denuncia en cuanto a temas digitales. De igual manera la brecha digital contribuye a esto, el desconocimiento genera un desinterés y con ello se queda a la deriva todo tema relacionado.

Ahora bien, las habilidades generadas a través de la tecnología son fundamentales para la sociedad donde la democratización tecnológica se ha convertido en una necesidad de supervivencia más allá de lo digital, no todo se queda en el uso de plataformas de internet, sino también en medios de comunicación a

través de los dispositivos. Por ello es necesario menciona al *smishing*, una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima —red social, banco, institución pública, etc.— con el objetivo de robarle información privada o realizarle un cargo económico (INCIBE, s. f.-b).

La brecha digital relacionada a la ciberseguridad también involucra dispositivos, en este caso los teléfonos móviles, que son el punto de conectividad, comunicación y uso preferido de la mayoría de los usuarios en México. Por ello, cualquier persona con brecha digital, podría caer en el engaño, al no saber si se trata de algo real o no, el fraude o estafa según sea el caso se podrían consumar, beneficiando al ciberdelincuente.

La ciberseguridad es una metodología que requiere atención a una escala social y de salud que ayude a la prevención de temas derivados del impacto psicológico posafectaciones. Por ejemplo, ante un ataque de *phishing*, que podría resultar en la divulgación sin consentimiento de información de un usuario, incluso lo llevaría a cometer suicidio, sin embargo, todo esto puede ser prevenible si focalizamos el problema.

A pesar de los grandes avances que la tecnología ha traído consigo, el problema de brecha digital se encuentra totalmente presente, las escalas de impacto requieren una atención mayor y todo podría comenzar con la publicación de este tipo de artículos para adentrar a la población a la temática relacionada.

## Conclusiones

A lo largo de este artículo hemos ido hilando el problema que deriva de la brecha digital y su relación básica con la ciberseguridad en un punto de desconocimiento que produce el engaño, y ahí las afectaciones a los usuarios.

La brecha digital es un problema latente no solamente en México, sino en el mundo, desafortunadamente no hay un combate frontal para ello, es aquí donde comenzamos desde la parte académica a dar visibilidad a este enemigo invisible para poder generar concientización en un primer momento.

El escenario es catastrófico al momento de tener una contemplación de alejamiento y hasta cierto punto discriminación hacia las poblaciones carentes de internet y TIC, el grado de vulnerabilidad es considerable, pues los ciberdelincuentes día a día evolucionan y se perfeccionan, trayendo consigo nuevos mecanismos de ataques digitales para inducir al engaño, particularmente dirigidos a blancos con factores de desconocimiento a la temática.

Partir de un entendimiento básico nos permitirá entender el contexto mayor y los distintos escenarios que pudieran derivarse de ello.

Reflexionemos como lectores. ¿Qué estamos haciendo para hacerle frente a la brecha digital?

Las múltiples respuestas podrían dar un punto de partida a generar debate, sin embargo, tengamos en cuenta que el primer punto es lograr un factor de concientización a los cercanos.

En materia de ciberseguridad revisar las comunicaciones de proveniencia, si se trata de *phishing*, *smishing* o cualquier variante, dudar en un primer momento y verificar si se trata de algo real o podría resultar en un tema fraudulento.

Existimos especialistas dispuestos a ayudar a toda persona que se acerque, pequeños esfuerzos ayudan a combatir a la brecha digital y prevenir en ciberseguridad.

## Referencias bibliográficas

Asociación Mexicana de Internet. (2023). *Estudio sobre los Hábitos de Usuarios de Internet en México 2023*. https://irp.cdn-website.com/81280eda/files/uploaded/19%20Estudio%20sobre%20los%20Hai-bitos%20de%20Usuarios%20de%20Internet%20en%20Mei-xico%202023%20.pptx.pdf

Chayko, M. (2016). *Superconnected: The Internet, Digital Media, and Techno-Social Life*. SAGE.

Domínguez, M. M. (2020). Digital inequality in Mexico: an analysis of the reasons for non-access and non-use of the internet. *Paakat: Revista de Tecnología y Sociedad*, *19*(10). https://doi.org/10.32870/pk.a10n19.519

INCIBE. (s. f.-a). *Phishing*. https://www.incibe.es/aprendeciberseguridad/phishing

INCIBE. (s. f.-b). *Smishing*. https://www.incibe.es/aprendeciberseguridad/smishing

Inkster, B., Knibbs, C., Bada, M. (2023). Cybersecurity: a critical priority for digital mental health. *Frontiers In Digital Health, 5*. https://doi.org/10.3389/fdgth.2023.1242264

Lisa, J. (2002). *Bridging the Digital Divide: Technology, Community and Public Policy*. Blackwell.

Ragnedda, M., Glenn, W. (2018). *Theorizing Digital Divides*. Routledge.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 87-98

# EL PELIGRO DE LA IRRELEVANCIA

*THE DANGER OF IRRELEVANCE*

**Juan Carlos Luna Barberena**

Abogado por la Universidad Panamericana.
Maestría por *Georgetown University Law Center*
Socio-Director y fundador de LAWIT by LAWGISTIC Group

## Resumen

El presente artículo trata de abordar la relevancia que las tecnologías digitales representan en un ámbito concreto como el legal desde la perspectiva empresarial y de competitividad, analizando los pros y los contras vinculados a su uso o falta de este. Para ello se abordan tecnologías que se están empleando en el ámbito privado y se estudia para qué, con el fin de valorar sus ventajas, problemas y aquellas que se podrían emplear en el corto plazo. Dado que el uso y la transformación tecnológica exigen formación, se presta también atención a la formación que en ese sentido sería conveniente tener en cuenta y, por tanto, también a los rasgos definitorios de los que podrían ser los líderes legales de los próximos años.



## Palabras clave

Tecnología, disrupción, competitividad, digitalización, innovación.



## Abstract

This article addresses the relevance that digital technologies represent in a specific field, such as the legal field, from a business and competitiveness perspective, analyzing the pros and cons linked to its use or lack thereof. For this purpose, technologies that are being used in the private sphere are addressed, as well as for what purposes they are used, to assess their advantages and problems, and those that could be used in the short term. Given that the use and technological transformation requires training, attention is also paid to training at university level. Therefore, this paper also pays attention to the features of those who could be the legal leaders of the coming years.



## Keywords

Technology, disruption, competitivity, digitalization, innovation.

## Introducción

En un mundo legal en constante evolución y transformación, ignorar los avances tecnológicos que puedan eficientar la forma de trabajar es el primer paso hacia la falta de competitividad y, en consecuencia, hacia la irrelevancia.

Entiendo por irrelevancia a aquella potencial situación en que un profesional del derecho deja de ser competitivo ante las crecientes exigencias y expectativas de brindar servicios legales de calidad, en forma eficiente y efectiva. Por eso, la urgencia de la transformación digital en la práctica legal es cada día más evidente, y da pie a la disrupción de todo el ecosistema legal y, en consecuencia, genera un reto importante hacia a adopción y adaptación de nuevas formas de gestionar todas las operaciones legales.

La interacción del abogado y la tecnología se analiza en muchas ocasiones desde una perspectiva de competitividad (Acens, 2008). Se ve como algo que le da valor agregado y no tanto como un deber ético. Es por ello que, en el mundo legal, se están dando interesantes discusiones sobre si el usar tecnología (García, 2023), y sobre todo entender cómo aplicarla, debería de ser un deber para los profesionales en derecho, independientemente de que sea una necesidad para mantenerse vigentes.

En la era de la digitalización, es decir, aquella época que abarca el inicio, apogeo y culminación de la revolución digital e informática de finales del siglo XX e inicios del XXI, donde cada aspecto de la economía y la sociedad está siendo transformado por la tecnología, el sector legal enfrenta una encrucijada crítica (Llamas, 2021). De ahí que la hipótesis de partida de este trabajo se base en la idea de que la resistencia a adoptar herramientas tecnológicas y la falta de avances hacia una disrupción digital no solo ponen en peligro la eficiencia y competitividad de los despachos de abogados y prácticamente de todo el ecosistema legal, sino que también amenazan con afectar la calidad y precisión de su trabajo y, por ende, relegar a la irrelevancia a aquellos profesionales que se nieguen a adaptarse.

Por ello, en este artículo se abordan los pros y los contras que el uso de tecnologías digitales o la falta de este pueden acarrear en el sector legal, tanto en perspectiva de la empresa, los despachos de abogados, como en la perspectiva de la formación que estos deben tener.

## La digitalización como imperativo estratégico

La práctica legal ha sido históricamente conservadora y cautelosa para adoptar cambios, con una fuerte dependencia en métodos tradicionales de gestión y análisis, y adversa al cambio. Sin embargo, el mundo contemporáneo exige mayor innovación, velocidad, agilidad y versatilidad, cualidades que solo pueden ser alcanzadas mediante la integración de tecnologías avanzadas a la práctica del derecho. Desde aspectos básicos de gestión, hasta llegar a implementar soluciones con inteligencia artificial y el análisis de datos masivos (*big data*), las herramientas tecnológicas tienen el potencial de transformar la manera en que

los abogados analizan, obtienen y procesan información, gestionan sus casos, interactúan con sus clientes y toman decisiones estratégicas.

Por lo tanto, el tema de transformación digital pasó en poco tiempo de ser algo opcional para convertirse en un requisito indispensable para mantener la relevancia de nuestras actividades (NTO, 2021).

## Eficiencia y agilidad: la demanda del cliente moderno

Ante las nuevas exigencias de los negocios, del comercio y la economía digital y del avance tecnológico de los demás sectores, los clientes actuales no solo buscan asesoría legal competente y con sólidos conocimientos técnicos y buena experiencia, sino que también demandan servicios rápidos, eficientes, proactivos y predictivos. La capacidad de procesar grandes volúmenes de información y de prever posibles escenarios legales mediante el uso de algoritmos predictivos puede ser la diferencia entre ganar o perder un caso. La implementación de sistemas de gestión de casos (*case management systems*), plataformas de colaboración en línea, y herramientas de análisis legal automatizado son solo algunos ejemplos de cómo la tecnología puede mejorar la eficiencia operativa, al tiempo que ayuda a prevenir riesgos.

## Proactividad y predicción: el nuevo paradigma legal

El enfoque reactivo tradicional del sector legal puede ser reemplazado por una postura más proactiva y predictiva. La inteligencia artificial, por ejemplo, permite a los abogados analizar patrones en datos legales históricos para prever resultados futuros, identificar riesgos potenciales y desarrollar estrategias más efectivas y mejor enfocadas y sustentadas. Estas capacidades no solo aumentan la probabilidad de éxito, sino que también fortalecen la relación con los clientes al ofrecerles un valor añadido significativo (GAMCO, 2023).

## La resistencia al cambio: un obstáculo peligroso

Pese a los evidentes beneficios que la tecnología ofrece, aún existe una resistencia considerable dentro del sector legal a adoptar estas herramientas. Esta resistencia no solo es un freno al progreso, sino que también representa una amenaza existencial para aquellos despachos y abogados que se niegan a innovar y evolucionar. En un entorno cada vez más competitivo, la falta de adaptación tecnológica puede resultar en la pérdida de relevancia (InnovAgile Group Spa, 2024), y en última instancia, en la obsolescencia profesional, por no estar a la altura de las nuevas exigencias.

## La urgencia de la capacitación continua

La transformación digital no es solo una cuestión de adoptar nuevas herramientas, sino también de desarrollar las habilidades necesarias para utilizarlas de manera efectiva. La capacitación continua en tecnologías emergentes debe

ser una prioridad para cualquier profesional del derecho que desee mantenerse relevante en el mercado legal. Programas de formación en inteligencia artificial, análisis de datos, y ciberseguridad son esenciales para asegurar que los abogados puedan aprovechar al máximo las oportunidades que la digitalización ofrece.

## Recomendaciones prácticas y ejemplos de tecnologías legales

Para facilitar la transición hacia una práctica legal más tecnológica, a continuación se presenta algunos ejemplos de las tecnologías aplicadas actualmente en el ámbito legal, con recomendaciones de cómo sacarle partido con base en las ventajas que se considera pueden representar para los despachos legales.

### 1. Sistemas de gestión de casos (Case Management Systems)

*Mejores prácticas*: implementar un CMS para centralizar la gestión de casos, documentos y comunicación con clientes.

*Ventajas*: mejora la organización, permite un acceso rápido a la información del caso, facilita la colaboración y reduce el tiempo dedicado a tareas administrativas.

### 2. Inteligencia artificial y aprendizaje automático

*Mejores prácticas*: utilizar herramientas para la investigación legal y el análisis de contratos.

*Ventajas*: acelera la investigación jurídica, identifica patrones en grandes conjuntos de datos, mejora la precisión y reduce el riesgo de errores humanos.

### 3. Análisis de datos (Big Data)

*Mejores prácticas*: integrar soluciones de análisis para prever resultados judiciales y tomar decisiones estratégicas basadas en datos históricos.

*Ventajas*: proporciona información valiosa sobre tendencias legales, ayuda a prever posibles resultados de litigios y optimiza la toma de decisiones.

### 4. Automatización de documentos

*Mejores prácticas*: utilizar *software* para automatizar la redacción y revisión de documentos legales.

*Ventajas*: aumenta la eficiencia, reduce el tiempo de preparación de documentos, y minimiza errores en la documentación.

### 5. Plataformas de colaboración en línea

*Mejores prácticas*: adoptar plataformas para mejorar la comunicación y colaboración entre los miembros del equipo legal.

*Ventajas*: facilita la comunicación en tiempo real, mejora la colaboración remota y asegura que todos los miembros del equipo estén alineados.

### 6. Soluciones de ciberseguridad

*Mejores prácticas*: implementar medidas robustas de ciberseguridad como el cifrado de datos y el uso de VPN para proteger la información sensible de los clientes.

*Ventajas*: garantiza la confidencialidad y seguridad de la información, protege contra ciberataques y cumple con las regulaciones de privacidad.

Todos estos sistemas en uso tienen en común que permitirían obtener un aumento de productividad laboral, si bien es cierto que su adopción a niveles amplios requerirá tiempo e inversión, y quizás lo más importante, un cambio cultural.

A futuro, será también la inteligencia artificial clave en el sector legal, por el impacto que puede llegar a suponer. En concreto, la IA generativa, como ChatGPT, tiene el potencial de transformar significativamente la profesión legal (Molina, 2023). A continuación, se presentan algunas formas de sus posibles impactos en el área de interés:

- *Automatización de tareas de bajo valor*: la IA generativa puede manejar tareas rutinarias y repetitivas, liberando a los abogados para que se concentren en trabajos más complejos y estratégicos. Por ejemplo, puede ayudar en la redacción de documentos legales, la realización de investigaciones jurídicas e incluso en la generación de borradores iniciales de casos.
- *Mejora de la investigación jurídica y la persuasión*: la IA puede analizar grandes cantidades de datos legales, identificar precedentes relevantes y proporcionar información para orientar el juicio de los abogados. También puede ayudar a crear argumentos más persuasivos al sugerir jurisprudencia y teorías legales relevantes.
- *Reducción de la brecha de acceso a la justicia*: las herramientas de IA pueden hacer que la información legal sea más accesible para el público, ayudando a reducir la brecha entre aquellos que pueden pagar por servicios legales y aquellos que no pueden. Por ejemplo, los *chatbots* pueden proporcionar orientación legal básica y dirigir a los usuarios a recursos relevantes.
- *Desafíos y consideraciones éticas*: aunque la IA generativa ofrece beneficios, también plantea preguntas éticas. Los abogados deben asegurarse de la precisión y fiabilidad del contenido generado por la IA. Además, deben protegerse contra *deepfakes* y pruebas falsas.

En resumen, la IA generativa está revolucionando a la práctica legal al agilizar procesos, mejorar la capacidad de la investigación y redefiniendo cómo los abogados abordan su trabajo. Sin embargo, requerirá una integración reflexiva y una supervisión continua para maximizar sus beneficios mientras se mantienen los estándares profesionales.

El *software* de IA ya está comenzando a demostrar que puede proporcionar asistencia en todas estas áreas, pero desde luego se irá evolucionando y avanzando en su conocimiento y uso conforme pase el tiempo. Lo que es claro es que la IA generativa irá transformando a la industria legal y todas sus aristas.

Los abogados se consuelan con la idea de que «una máquina nunca podrá reemplazarnos» en el ejercicio del juicio profesional y el compromiso interpersonal (Bonina, 2023). Pero incluso para esos deberes sagrados se avecina un cambio. Las cuatro competencias funcionales principales para la industria legal, y de hecho para muchos profesionales, son la persuasión, la creación de contenido, el juicio y el conocimiento, en todas ellas, un soporte importante estará basado en soluciones tecnológicas para reforzarlas y aumentar sus capacidades.

La IA jugará un papel cada vez más central en el desempeño de todas estas competencias, y no solo en el conocimiento y la creación de contenido, que son el foco actual de la industria. A medida que los conjuntos de datos disponibles crezcan, y a medida que los profesionales y proveedores de servicios inviertan en el diseño y construcción de nuevos casos de uso, la capacidad de los sistemas de IA para acumular, organizar, resumir, extraer y tamizar información aumentará la forma en que los abogados gestionan sus actividades.

La capacidad de la IA para mejorar la productividad no debe eclipsar la importancia de las cualidades humanas. La voluntad de aprender, la intención de mejorar, la capacidad de adaptarse y la interpretación correcta de factores contextuales no evidentes (por ejemplo, la incidencia de la cultura de las partes en una negociación internacional) son atributos que ninguna máquina puede replicar completamente.

Los abogados más exitosos serán quienes no solo dominen las herramientas tecnológicas disponibles, sino que también posean la capacidad de aplicar el conocimiento de manera creativa y estratégica (Pérez Alonso, 2018). La IA puede asistir en el análisis y la gestión de información, pero la interpretación de los datos y la toma de decisiones acertadas requieren un juicio humano que va más allá de los algoritmos.

En última instancia, la IA debe ser vista como una poderosa herramienta que complementa y amplifica las habilidades humanas, y no como un sustituto de estas. La clave del éxito en la era digital radica en encontrar un equilibrio entre la tecnología, de un lado, y el talento y la experiencia humana, de otro, asegurando que ambos trabajen en armonía para alcanzar los mejores resultados posibles.

## Consecuencias negativas de no adoptar tecnologías legales

La falta de adopción de herramientas tecnológicas puede tener efectos adversos para un despacho de abogados o un departamento legal corporativo (Benedet, 2019). A continuación, se analizan algunas de las consecuencias negativas derivadas del no uso de estas tecnologías.

*1. Pérdida de competitividad*: aquellos despachos y equipos legales corporativos que no adoptan tecnologías avanzadas no podrán competir eficazmente con

aquellos que sí lo hacen. El menor grado de eficiencia y agilidad que ello puede suponer puede resultar en la pérdida de clientes a favor de competidores más tecnológicos.

*2. Reducción en la eficiencia operativa*: la dependencia de métodos manuales y tradicionales ralentiza los procesos legales. Ello supone horas de trabajo, un incremento de los costos operativos y, en consecuencia, tiempos de respuesta prolongados conectados con los problemas de capacidad derivados de manejar grandes volúmenes de trabajo. Se convierte en un efecto adverso en relación con la agilidad y velocidad con que trabajan las máquinas y aquellos que las empleen.

*3. Menor capacidad de análisis y predicción*: sin herramientas de análisis de datos e inteligencia artificial, la capacidad de prever resultados y mitigar riesgos por parte del humano es limitada. En consecuencia, quizás las estrategias legales resultan menos informadas o incompletas que las inspiradas o basadas en mecanismos de Inteligencia artificial, además de correr el riesgo de contar con una mayor probabilidad de errores.

4. Débil Protección de Datos: La falta de medidas robustas de ciberseguridad expone a los despachos y equipos legales corporativos a riesgos de seguridad. Si bien la seguridad total no existe, la vulnerabilidad a ciberataques y violaciones de datos será un problema a afrontar que corre el riesgo de conllevar una pérdida de confianza de los clientes, si se constatan defectivamente vulneraciones como las descritas.

*5. Insatisfacción del cliente*: los clientes actuales esperan servicios rápidos, eficientes y seguros. La incapacidad de cumplir con estas expectativas puede resultar en una disminución de la satisfacción y fidelización del cliente con el servicio legal prestado.

*6. Obsolescencia profesional*: los abogados que no se capaciten en nuevas tecnologías corren el riesgo de quedarse atrás, y perder competitividad. Se tendrán que afrontar las dificultades para adaptarse a las nuevas realidades del mercado laboral, teniendo en cuenta que ante la falta de adaptación se puede producir una disminución de oportunidades del crecimiento profesional.

## La relevancia de la transformación en la formación académica

La adopción de tecnologías legales no debe limitarse a la práctica profesional, es igualmente crucial que el ámbito académico y de formación de abogados también adopte cambios fundamentales en sus planes y esquemas de formación y capacitación. Es vital la inclusión de materias enfocadas en la innovación legal, el manejo de proyectos, la gestión y operación legal, y el uso de herramientas de análisis de datos y de inteligencia artificial.

Varias universidades líderes a nivel mundial ya están implementando cursos y especializaciones que integran estas áreas (Herrera, 2021). La formación de abogados más conocedores de herramientas *legaltech* y de nuevos modelos de gestión se considera indispensable para preparar a los profesionales del derecho para una economía cada vez más digitalizada.

En referencia a ello, podemos mencionar algunos de los aspectos básicos que debieran ser considerados para incluirse en los sistemas de enseñanza del derecho:

*Integración del* «*legaltech*», incluyendo en los planes de estudio módulos específicos sobre tecnologías legales, como inteligencia artificial aplicada al derecho y análisis de datos.

*Manejo de proyectos y gestión legal*, ofreciendo cursos que enseñen habilidades en gestión de proyectos legales y operaciones.

*IA, ciberseguridad y ética*, para tratar de conseguir que los estudiantes comprendan los aspectos regulatorios y éticos relacionados con la tecnología legal y la inteligencia artificial.

*Relación con ecosistemas digitales*, fomentando la colaboración con empresas de tecnología y *startups* para proporcionar a los estudiantes experiencia práctica en entornos de transformación digital.

## Perfil de los líderes en la transformación digital del sector legal

La transformación digital en el sector legal no solo requiere herramientas tecnológicas, sino también un cambio profundo en la mentalidad y perfil de los abogados que lideran esta revolución. Estos líderes no solo deben entender la importancia de la tecnología, sino que también deben estar impulsados por una visión clara de cómo se puede transformar y mejorar la práctica del derecho. A continuación, se analiza el perfil que opinamos deben tener estos pioneros, sus motivaciones, estrategias y el impacto tangible de sus acciones en el sector legal.

En concreto, estos abogados creemos que deben contar con varias características clave, entre las que destacan las siguientes:

*Curiosidad Intelectual*: deben estar constantemente buscando nuevas maneras de mejorar sus prácticas mediante la adopción de nuevos procesos y la adopción de nuevas tecnologías.

*Adaptabilidad*: han de ser capaces de adaptarse rápidamente a los cambios y no temer experimentar con nuevas herramientas.

*Visión estratégica*: han de tener capacidad para comprender cómo la tecnología puede integrarse en su práctica diaria para mejorar la eficiencia y los resultados de su trabajo.

*Habilidades interdisciplinarias*: han de saber combinar conocimientos legales con habilidades en gestión de proyectos, análisis de datos y tecnología de la información.

Estos abogados del futuro inminente, para ser líderes en transformación digital del sector legal[1], opinamos que deben contar con una motivación específica que pasa por querer, en primer lugar, mejorar la eficiencia, buscando reducir el tiempo y los costos asociados con la práctica legal mediante la automatización y la optimización de procesos; en segundo lugar, mantener o incrementar

1 Ver, con carácter general: Contact Center Hub (2022).

la calidad del servicio, ofreciendo un mejor servicio al cliente mediante el uso de herramientas que permiten una asesoría más rápida y precisa; en tercer lugar, ser competitivos, entendiendo que un elemento de competitividad es la tecnología, por las ventajas que conlleva; y en cuarto lugar, estar en continua actualización o innovación, mejorando sus prácticas mediante el uso de tecnologías emergentes.

Estos perfiles y sus prácticas adecuadas a la era digital no solo podrán mejorar la eficiencia operativa y la calidad del servicio, sino que también creemos que podrán tener un impacto directo en los resultados financieros y el reconocimiento profesional de los abogados a título personal y también en cuanto entidad corporativa. Como resultados concretos en este sentido prevemos que se podrá conseguir: un mayor retorno de inversión, en tanto que la implementación de tecnología reduce los costos operativos y aumenta la productividad; una expansión de la base de clientes, dada la capacidad de ofrecer servicios más rápidos y precisos, atrayendo a más clientes y aumentando la fidelización; el reconocimiento en el mercado, siendo vistos como líderes innovadores en el sector los despachos más tecnológicos, resultando atractivos en el mercado al menos para ciertos sectores.

## Ganar sobre realidades cambiantes

Si hay una lección que hemos aprendido de la pandemia, es que el abogado (dentro de cualquier ámbito de actividad) debe mantenerse flexible al responder a eventos que cambian rápidamente. Después de la pandemia, en general los dueños de empresas, CEO y juntas directivas no buscan un asesor jurídico tradicional, un buen abogado técnico, o una persona que simplemente diga sí en sus equipos, ni alguien que solo se enfoque en asuntos legales. Quieren que su asesor jurídico y los miembros del equipo legal sean facilitadores del negocio mientras manejan las circunstancias cambiantes en forma ágil, responsable, preventiva y proactiva.

El cliente empresarial quiere abogados y profesionales que puedan impactar el negocio de una manera significativa y valiosa, enfocándose en los ingresos, costos y riesgos. Realmente quieren resultados que impacten el negocio y que se puedan ver y medir. Y es precisamente en tal intersección donde es necesario que cualquier asesor jurídico sea un líder, que pueda combinar conocimiento y experiencia, con adaptabilidad, resiliencia e innovación, todo bajo el aura de una realidad disruptiva para el negocio y para el negocio del derecho.

Eso es lo que importa en el entorno global competitivo y cambiante de hoy. No son los más fuertes ni los más inteligentes los que sobrevivirán, sino aquellos que mejor puedan gestionar el cambio.

## Conclusiones

La adopción de herramientas tecnológicas en el ámbito legal no es solo una ventaja competitiva, sino una necesidad imperativa para los abogados en el mundo moderno. Las tecnologías avanzadas como la inteligencia artificial, el

análisis de datos, y las plataformas de gestión de casos permiten a los abogados manejar grandes volúmenes de información con mayor precisión y eficiencia, reduciendo el riesgo de errores humanos y agilizando procesos complejos. Esto no solo mejora la productividad, sino que también proporciona un servicio más rápido y de mayor calidad a los clientes.

Además, las herramientas tecnológicas facilitan la colaboración y la comunicación, tanto dentro de las firmas legales, y áreas legales corporativas, como con los clientes, permitiendo un flujo de trabajo más transparente y mejor coordinado. En un entorno donde la competencia es feroz y las expectativas de los clientes son cada vez más altas, la capacidad de adaptarse y adoptar nuevas tecnologías se traduce en una ventaja significativa.

En resumen, el uso de herramientas tecnológicas es crucial para que los abogados se mantengan relevantes y eficientes en un mercado en constante evolución. Ignorar estas herramientas no solo significa quedarse atrás, sino también arriesgarse a ofrecer un servicio inferior en un mundo donde la excelencia y la innovación son más accesibles y esperadas que nunca

La transformación digital es inevitable y aquellos que se aferren a métodos tradicionales corren el riesgo de quedar atrás. Los abogados deben reconocer que la adopción de tecnologías avanzadas no es una opción, sino una necesidad estratégica para sobrevivir y prosperar en una economía cada vez más digital. Solo aquellos que abracen el cambio y se adapten a las nuevas realidades podrán ofrecer servicios legales que estén a la altura de las exigencias modernas, manteniendo así su relevancia y competitividad en el futuro.

La tecnología no es el enemigo; la resistencia al cambio sí lo es. Es hora de que el sector legal abrace plenamente la disrupción digital y transforme sus prácticas para enfrentar con éxito los desafíos del mañana. La educación jurídica también debe evolucionar para preparar a las futuras generaciones de abogados, asegurando que tengan las herramientas y conocimientos necesarios para liderar en un mundo digital. Al hacerlo, no solo mejorarán sus prácticas, sino que también contribuirán a un sistema legal más eficiente, equitativo y accesible.

## Referencias bibliográficas


Acens. (2008). La competitividad que aporta la tecnología al mundo de la abogacía. *Blog Acens*. https://blog.acens.com/general/la-competitividad-que-aporta-la-tecnologia-al-mundo-de-la-abogacia/

Benedet, M. (2019). Consecuencias de la inteligencia artificial para el sector legal. *LemonTech Blog*. https://blog.lemontech.com/consecuencias-inteligencia-artificial-para-sector-legal/

Bonina, N. (2023). ¿Las máquinas reemplazarán a los abogados? *The Next Legal*. https://www.linkedin.com/pulse/las-m%C3%A1quinas-reemplazar%C3%A1n-los-abogados-nicol%C3%A1s-bonina/

Contact Center Hub. (2022). ¿Cuáles son los líderes de la transformación digital? *Contact Center Hub*. https://contactcenterhub.es/cuales-son-lideres-transformacion-digital-2022-17-38268/

GAMCO. (2023). Por qué la IA predictiva es clave para el éxito de una empresa. *GAMCO, Predict & Act*. https://gamco.es/la-ia-predictiva-clave-para-el-exito-de-una-empresa/

García, S. (2023). Érase una vez la abogacía y el uso de la tecnología para proporcionar servicios legales. *Unir*. https://www.unir.net/derecho/revista/la-abogacia-y-el-uso-de-las-legaltech-tecnologia-para-proporcionar-servicios-legales/

Herrera, F. (2021). ¿Dónde estudiar Legaltech? *Confilegal*. https://confilegal.com/20210312-opinion-donde-estudiar-legaltech/

InnovAgile Group Spa. (2024). Los riesgos de no adaptarse a la innovación tecnológica. *InnovAgile Group Spa. https://innovagilegroup.cl/f/los-riesgos-de-no-adaptarse-a-la-innovaci%C3%B3n-tecnol%C3%B3gica*

Llamas, J. (2021). Era digital. *Economipedia*. https://economipedia.com/definiciones/era-digital.html#:~:text=La%20era%20digital%20es%20aquella,inform%C3%A1tica%20y%20las%20herramientas%20digitales.

Molina, S. (2023). La Inteligencia Artificial generativa en el sector legal. *Blog de Innovación Legal y Nuevas Tecnologías*. https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/la-inteligencia-artificial-generativa-en-el-sector-legal/

NTO. (2021). Transformación digital de las administraciones tributarias. *Segunda Conferencia técnica de la NTO*. https://www.nto.tax/es/news/transformacion-digital-de-las-administraciones-tributarias

Pérez Alonso, G. (2018). Los despachos de abogados más exitosos serán los que salgan al encuentro del cambio y animen al cliente a adoptarlo, acompañándoles en el camino. *Abonomics. https://blog.lexgoapp.com/los-despachos-abogados-mas-exitosos-seran-los-salgan-al-encuentro-del-cambio-animen-al-cliente-adoptarlo-acompanandoles-camino/*

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 99-107

# LAS OBLIGACIONES DE TRANSPARENCIA PARA ELIMINAR LOS RIESGOS DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

*TRANSPARENCY OBLIGATIONS TO ELIMINATE THE RISKS OF ARTIFICIAL INTELLIGENCE SYSTEMS*

**Elisa Palomino Angeles**

Universidad Autónoma Metropolitana

## Resumen

Con la evolución de los sistemas de inteligencia artificial, se ha masificado una diversidad de riesgos, por ello, el Parlamento Europeo crea un Reglamento Europeo sobre Inteligencia artificial, en el cual se establecen normas armonizadas en la materia, en la cual, de acuerdo al enfoque del riesgo, se clasifican los riesgos en inaceptables, de alto riesgo, riesgo limitado y riesgo bajo o mínimo. Asimismo, se contemplan los riesgos genéricos y sistémicos, y se regulan las obligaciones de transparencia, las cuales analizamos como nuestro objeto de investigación para poder determinar si existen lagunas, incoherencias o problemas semánticos que hagan a la norma ineficaz para eliminar los riesgos que se originan con el uso de la inteligencia artificial. Entre esas obligaciones encontramos que el proveedor deberá informar al usuario que está interactuando con un sistema de IA, excepto cuando sea evidente que lo está haciendo con una persona física, razonablemente informada, atenta y perspicaz teniendo en cuenta las circunstancias y contexto.



## Palabras clave

Obligaciones, transparencia, riesgos, inteligencia artificial.



## Abstract

With the evolution of artificial intelligence systems, a diversity of risks has become widespread, therefore, the European Parliament created a European Regulation on Artificial Intelligence, which establishes harmonized rules on artificial intelligence, in which risks are classified as unacceptable, high risk, limited risk, and low or minimal risk. Likewise, generic and systemic risks are contemplated, and transparency obligations are regulated, which we analyze as our object of research in order to determine if there are gaps, inconsistencies or semantic problems that may cause the regulation to be ineffective in eliminating the risks that arise from the use of artificial intelligence. Among these obligations, we find that the provider must inform the user that he or she is interacting with an AI system, except when it is evident that you are doing so with a natural person, reasonably informed, attentive and discerning taking into account circumstances and context.



## Keywords

Obligations, transparency, risks, artificial intelligence.

## Introducción

En la actualidad, la complejidad digital de los sistemas provoca que se presenten más dificultades para desarrollar sistemas jurídicos que nos permitan contar con el mínimo de protección de los usuarios o consumidores de los sistemas de inteligencia artificial. Hoy se requieren normas eficaces en las cuales se pueda establecer instrumentos jurídicos que materialicen las obligaciones de la transparencia que les corresponde a los proveedores de sistemas de inteligencia artificial, como un derecho para eliminar algunos de sus riesgos. ¿Cuáles son las obligaciones que evitarán o eliminarán los riesgos de uso y aplicación de los sistemas de inteligencia artificial? ¿Se podrá establecer la igualdad o equidad en las relaciones asimétricas que hoy se presentan entre los usuarios y los proveedores de estos sistemas? Es la capacidad económica de los sujetos en esta relación asimétrica uno de los elementos que favorece la desigualdad entre los mismos proveedores en relaciones desiguales.

## La inteligencia artificial

El sistema de inteligencia es una complejidad digital en la que interactúa una diversidad de elementos, tecnologías digitales, sujetos, instituciones, gobiernos, la entropía que producen estas relaciones jurídicas, tanto simétricas como asimétricas, la cual ha originado una necesidad de establecer modelos de seguridad para los sistemas de inteligencia artificial, en los cuales las normas sean eficaces de tal manera que no se vulneren derechos fundamentales.

En ese orden de ideas tenemos que iniciar primero con los aspectos fundamentales, como son algunas definiciones del Reglamento Europeo de Inteligencia Artificial (Ley sobre Inteligencia Artificial), promulgado el 13 de marzo de 2024 por el Parlamento Europeo, el cual establece la definición legal de inteligencia artificial de la siguiente manera:

> A los efectos del presente Reglamento, se entenderá por: 1) «sistema de IA»: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales. (Art. 3.1).

Uno de los problemas ha sido definir qué es un sistema de inteligencia artificial, porque existe una multiplicidad de significados desde diversas perspectivas: jurídica, económica, y tecnológica, y es en la Ley sobre Inteligencia Artificial del Parlamento Europeo que se establece la referida definición legal, la cual fue cuestionada por la Big Data Value Association,

> una organización internacional sin ánimo de lucro impulsada por la industria. Subrayó que la definición de sistemas de IA era bastante amplia y abarcaría mucho más de lo que se entiende subjetivamente como IA, incluidos los algoritmos de búsqueda, clasificación y enrutamiento más simples, que en consecuencia estarían sujetos a nuevas reglas. (Parlamento Europeo, 2024).

De lo que se desprende que se incluye más sistemas de inteligencia artificial, e incluso las de más bajo nivel, contemplados en la referida ley, pero también encontramos la el argumento de AmCham, la Cámara de Comercio Americana en la UE, que sugirió

> evitar el exceso de regulación mediante la adopción de una definición más estrecha de los sistemas de IA, centrándose estrictamente en las aplicaciones de IA de alto riesgo (y no extendida a las aplicaciones de IA que no son de alto riesgo, o al *software* en general). (Parlamento Europeo, 2024).

Por lo que se puede desprender que puede ser muy amplia la definición de inteligencia artificial, y en este caso se pretende evitar un exceso de regulación a sistemas de inteligencia con mínimo riesgo.

Es interesante lo que refiere AmCham porque los expertos en los sistemas inteligentes pueden realizar una clasificación de estos, pero hay que considerar que esa multiplicidad de sistemas no solo se debe clasificar de acuerdo al riesgo, sino que también se debe considerar más categorías, como la potencia del sistema y el nivel de autonomía para alcanzar metas, la capacidad de aprender, de adaptarse, es decir, aquellas que tomen decisiones sin control y con alto riesgo, porque no todo es inteligencia artificial.

## Tipos de riesgos

En el referido Reglamento Europeo se regula las definiciones de riesgo, que se entiende como la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio (art. 3. inciso 2), se tiene que determinar el daño causado y la gravedad de este para poder determinar su pago de indemnización, que es considerado como genérico, ahora entendemos como «perjuicio la privación de cualquier ganancia lícita, que debiera haberse obtenido con el cumplimiento de la obligación» (México, Suprema Corte de Justicia, 1967). Es decir, una lesión al patrimonio de los usuarios o consumidores de sistemas de inteligencia artificial, donde la responsabilidad, tanto civil como penal, deberá reparar el perjuicio; y, por otra parte, el término gravedad como la importancia que tiene el perjuicio.

Ahora bien, también se regula el «riesgo sistémico»:

> un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor.

En este orden de ideas, el Parlamento Europeo, con base en el riesgo, regula la clasificación de estos, entre los cuales incluye: a) riesgos inaceptables o prohibidos, b) sistemas de inteligencia artificial con alto riesgo, c) sistemas de inteligencia artificial con especificaciones, y d) sistemas de inteligencia artificial con mínimo riesgo o sin riesgo. De ellos, solo mencionaremos a los dos primeros por su trascendencia.

*a) Riesgo inaceptable*:

> (…) los sistemas de IA de riesgo inaceptable son los que se consideran una amenaza para las personas y serán prohibidos. Incluyen:
>
> Manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos: por ejemplo, juguetes activados por voz que fomentan comportamientos peligrosos en los niños
>
> Puntuación social: clasificación de personas en función de su comportamiento, estatus socioeconómico o características personales Sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial (…). (Parlamento Europeo, 2023).

Además, en relación con el art. 1, el art. 5 regula las «Prácticas de IA prohibidas»:

> 1. Quedan prohibidas las siguientes prácticas de IA: a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un grupo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que una persona tome una decisión que de otro modo no habría tomado, de un modo que provoque, o sea probable que provoque, perjuicios considerables a esa persona, a otra persona o a un grupo de personas (…). (Parlamento Europeo, 2024).

Es un acierto el haber prohibido la manipulación cognitiva y salvaguardado la libertad de expresión, el consentimiento informado y la salud mental del individuo. Resulta acertado y necesario establecer excepciones en el caso de los sistemas de identificación biométrica en tiempo real y a distancia, sobre todo tratándose de casos de seguridad pública.

*b) Sistemas de inteligencia artificial con alto riesgo*: son aquellos permitidos al sujeto siempre que cumpla los requisitos del reglamento de IA y la evaluación de conformidad (Ministerio de Asuntos Económicos y Transformación Digital, s. f.).

*c) Sistemas de inteligencia artificial con especificaciones:* son aquellos permitidos pero, tanto proveedores como usuarios, están sujetos a cumplir con la transparencia.

*d) Sistemas de inteligencia artificial con mínimo riesgo o sin riesgo*: son aquellos permitidos.

## Las obligaciones de transparencia como elementos para eliminar los riesgos en los sistemas de IA

El derecho a la información es un derecho fundamental que genera obligaciones de transparencia por parte de proveedores y usuarios, pero ¿qué entendemos por transparencia? De acuerdo con la OCDE, la transparencia es un concepto relacionado con la posibilidad de que la información real de una empresa, gobierno u organización sea consultada por los diferentes sujetos afectados por

ella, de tal modo que estos puedan tomar decisiones con conocimiento de causa y sin asimetría de información (Perramon, 2013).

En el Título IV, artículo 50, «Obligaciones de transparencia de los proveedores y usuarios de determinados sistemas de IA», se señala:

> 1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de forma que las personas físicas de que se trate estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por ley para detectar, prevenir, investigar o enjuiciar infracciones penales, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar una infracción penal.

Es importante resaltar que este artículo se refiere a la interacción que tiene las personas físicas con un sistema de inteligencia artificial, en la cual la transparencia consiste en que el proveedor deberá informar que se está interactuando con un sistema de IA, a menos de que la interacción sea con un individuo razonablemente informado, atento y perspicaz, teniendo en cuenta su entorno y particularidades.

Consideremos que son ambiguas las palabras que se utilizaron como candados: tener una observación aguda y penetrativa, razonablemente informada, que una persona esté acorde a su edad y escolaridad, una visión aguda y penetrativa o extremadamente observadora (Real Academia Española, s.f.).

¿Qué parámetros se necesita para determinar la obligación de transparencia que deben tener los proveedores? En las relaciones asimétricas, como es el caso que nos ocupa, entre usuarios y proveedores, se requiere darles mayores derechos a los usuarios, por las desventajas económicas y de conocimiento que existen entre ellos. Aunado a que se requiere de conocimiento tecnológico muy especializado para poder ser razonablemente informado, esto conlleva el conocimiento de expertos, por ejemplo: no se podrá detectar que se está hablando con una máquina de IA y no con un humano, porque se pueden reproducir las voces humanas sin que la persona se percate de la situación.

Continuando con el análisis del número 2 del art. 50 referido, tenemos que dice:

> 2. Los proveedores de sistemas de IA, entre los que se incluyen los sistemas de IA de uso general, que generen contenido sintético de audio, imagen, vídeo o texto, velarán por que la información de salida del sistema de IA esté marcada en un formato legible por máquina y que sea posible detectar que ha sido generada o manipulada de manera artificial. Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA desempeñen una función de apoyo a la edición estándar

> o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica, o cuando estén autorizados por ley para detectar, prevenir, investigar o enjuiciar infracciones penales. (Parlamento Europeo, 2024).

Este se refiere a la obligación de transparencia que tiene el proveedor de los sistemas de inteligencia artificial de uso general que generan contenido sintético de audio, imagen, video o texto. Dice que «velará», consideramos que no es la palabra adecuada, más bien es «vigilará», aunque no se utiliza esta palabra, sino que velará por que la información del sistema de IA de salida esté marcada por el proveedor en formato legible y detectable sobre la generación o manipulación artificial, esto es un gran acierto, pero resulta ser que, como en el punto anterior, se establece una diversidad de excepciones que no tienen un lenguaje sencillo para el usuario, sino para los expertos en sistemas de inteligencia artificial, y nuevamente se utiliza excepciones a las reglas generales, lo cual podrá dar lugar a evadir responsabilidades. En las excepciones están la edición estándar o modificación sustancial de los datos de entrada.

«El formato legible por máquina y que sea posible detectar que ha sido generada o manipulada de manera artificial»: al proveedor, en esta frase, se le da la posibilidad, mas no la obligación, de tener un formato que detecte que la información ha sido generada o manipulada de manera digital, es deber tener una solución técnica viable, eficaz interoperable, sólida. Consideramos que estos requisitos deberán estar establecidos dentro de las normas técnicas pertinentes, los estándares internacionales no deberán estar sujetos a la posibilidad del proveedor, si realmente se quiere prevenir el riesgo informático, ya que si bien es cierto que existen diversas empresas de distintos niveles económicos y tecnológicos, también es cierto que será necesario tener un fondo económico para apoyar o financiar a pequeñas empresas para que puedan cumplir con estas obligaciones de transparencias.

Observamos que al establecer en la medida que sea «técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual», se ayudará los proveedores de pymes, lo cual fomentará la inalterabilidad de los datos de entrada facilitados por el responsable.

> 3. Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él y tratarán sus datos personales de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y con la Directiva (UE) 2016/680, según corresponda. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones que hayan sido autorizados por ley para detectar, prevenir e investigar infracciones penales, con sujeción a las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la Unión. (Parlamento Europeo, 2024).

En este punto tres, en los sistemas de reconocimientos de emociones o categorización biométrica, el responsable deberá informar del despliegue sobre su funcionamiento a las personas expuestas.

> 4. Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrafalsificación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial (…). Los responsables del despliegue de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público divulgarán que el texto se ha generado o manipulado de manera artificial. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar o enjuiciar infracciones penales, o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido. (Parlamento Europeo, 2024).

Generación o manipulación de imágenes, audio, video o *deepfakes*: información pública sobre su origen artificial. Si se trata de informar al público sobre asuntos de interés público, el responsable del despliegue debe informar sobre su origen salvo que haya supervisión humana o control editorial y una persona tenga responsabilidad editorial por la publicación.

Información suministrada de manera clara y distinguible en las primeras interacciones y exposiciones: es muy acertado el regular esta obligación de transparencia a la inteligencia generativa, debido a las conductas ilícitas que se pueden generar con el mal uso de esta.

## Conclusiones

La transparencia específica sólo aplica a los sistemas de inteligencia artificial generativa, consideramos que deberá revisarse la clasificación de los sistemas de IA para proteger a los usuarios, que son los más vulnerables en esta cadena de valores. Además, si bien es cierto que establece obligaciones tanto para los proveedores como para los responsables del despliegue, las cuales consideramos que son pertinentes, también es cierto que establece muchas excepciones a las obligaciones, por las cuales se podrá evadir la responsabilidad civil o penal, debido a que algunas de estas normas son insuficientes, vagas y ambiguas. Las obligaciones de transparencia pueden ser eficaces si se perfeccionan las normas, sobre todo las excepciones a la regla general.

## Referencias bibliográficas

México. Suprema Corte de Justicia. (1967). *Diferencia entre daño y perjuicio*. https://sjf2.scjn.gob.mx/detalle/tesis/258965

Ministerio de Asuntos Económicos y Transformación Digital. (s. f.). *El Reglamento Europeo de IA, en resumen*.

https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf

https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial

https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2021)698792

https://accid.org/wp-content/uploads/2018/10/La_transparencia._Concepto_evolucion_y_retos_a.pdf

Parlamento Europeo. (2023). *Ley de IA de la UE: primera normativa sobre inteligencia artificial*. https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial

Parlamento Europeo. (2024). *Artificial Intelligence Act*. https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2021)698792

Perramon, J. (2013). La transparencia: concepto, evolución y retos actuales. *Revista de Contabilidad y Dirección*, *16,* 11-27. https://accid.org/wp-content/uploads/2018/10/La_transparencia._Concepto_evolucion_y_retos_a.pdf

Real Academia Española. (s. f.). Perspicacia. *Diccionario de la lengua española*. https://dle.rae.es/perspicacia

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 109-121

# IA Y SESGOS: UNA VISIÓN ALTERNATIVA EXPRESADA DESDE LA ÉTICA Y EL DERECHO

*AI AND BIAS: AN ALTERNATIVE VIEW FROM ETHICS AND LAW*

**Fernando López Martínez**
**José Heriberto García Peña**

Abogados y profesores de Innovación Tecnológica
del Derecho, Tecnológico de Monterrey

## Resumen

Este artículo pretende examinar, desde la deontología jurídica, los sesgos algorítmicos en la inteligencia artificial (IA) y su impacto en diversas aplicaciones. Se analiza cómo estos sesgos pueden surgir, las consecuencias negativas que pueden tener y las posibles soluciones para mitigarlos. A través de una revisión de la literatura y el análisis de casos prácticos, este estudio destaca la importancia de abordar los sesgos para garantizar la equidad y la justicia en el uso de IA. Se profundiza en ejemplos específicos en sectores como la salud, el empleo y la justicia, y se discuten las implicaciones éticas y sociales de los sesgos de IA en sectores considerados más vulnerables incluyendo el género, como es el caso de la población de la diversidad sexual, en particular las personas LGBTIQ+. Finalmente, se busca participar en la discusión y análisis bajo una visión ética y jurídica, matizando algunas propuestas a seguir.



## Palabras clave

Inteligencia artificial, sesgos, algoritmos, equidad, ética, justicia.



## Abstract

This paper examines, from the perspective of legal deontology, algorithmic biases in artificial intelligence (AI) and their impact on various applications. It analyzes how these biases can arise, their potential negative consequences, and possible solutions to mitigate them. Through a review of the literature and the analysis of practical cases, this study highlights the importance of addressing biases to ensure fairness and justice in the use of AI. Specific examples in sectors such as healthcare, employment, and justice are explored, and the ethical and social implications of AI biases in more vulnerable sectors, including gender and the LGBTQ+ community, are discussed. Finally, the article seeks to participate in the discussion and analysis from an ethical and legal perspective, outlining some proposals to follow.



## Keywords

Artificial intelligence, biases, algorithms, equity, ethics, justice.

*La inteligencia artificial (…) puede ser (…) sexista y racista. Es hora de volverla justa.*

James Zou y Londa Schiebinger (2018, p. 32)

## Introducción

> (…) Quería aprender a hacer tecnología que fuera interesante. Así que vine al MIT y trabajé en proyectos de arte que usaban visión artificial (…). Lees ciencia ficción y eso te inspira a crear algo que seguramente sería poco práctico si no tuvieras el curso como excusa para hacerlo. Yo quise construir un espejo que me inspirara por las mañanas. Lo llamé Espejo Aspire (…). Le coloqué una cámara y con un software de visión artificial, se suponía que debía detectar los movimientos de mi cara. Pero el problema era que no funcionaba bien, hasta que me puse una máscara blanca.
>
> Cuando me ponía la máscara, me detectaba. Cuando me la quitaba, ya no me detectaba[1].

Las aproximaciones de principios de siglo sobre la administración electrónica se han visto ampliamente superadas por los hechos actuales, más tras la pandemia, cuando el uso de todo tipo de tecnologías se intensificó sobremanera. Entonces la toma de decisiones estuvo muy condicionada por los modelos matemáticos de predicción de la incidencia previsible, a partir de datos de movilidad y patrones identificados por las máquinas, interpretadas por especialistas.

Toda innovación plantea en sus etapas tempranas fallos de precisión y descubrimiento de desventajas, contratiempos que son corregidos con la lógica de ensayo y error. Nunca ninguna tecnología se incorporó a la sociedad sin controversias, contratiempos y discusiones, y siempre se abrieron debates sobre sus potenciales riesgos y daños para el ser humano. Esto que hoy sucede con la inteligencia artificial, antes sucedió con la electricidad, el ferrocarril o los teléfonos móviles.

La inteligencia artificial ha transformado múltiples sectores, desde la atención médica hasta el comercio, ofreciendo numerosas ventajas en términos de eficiencia y precisión. Sin embargo, la IA no está exenta de problemas, uno de los más significativos es el sesgo algorítmico. El objetivo del artículo es explorar la naturaleza de estos sesgos, sus causas y efectos, y discutir estrategias para mitigarlos. Se presenta un marco conceptual sobre el sesgo algorítmico bajo una visión ética y jurídica, y se plantea como pregunta central de investigación: ¿cómo pueden los desarrolladores y usuarios de IA identificar y reducir los sesgos algorítmicos?

1 Así comienza *Prejuicio Cifrado* (*Coded Bias*), el documental dirigido por la cineasta Shalini Kantayya y estrenado en 2020 que narra cómo la investigadora Buolamwini tomó conciencia del sesgo racial existente en los algoritmos de reconocimiento facial y analiza sus consecuencias. Joy Buolamwini es una mujer negra, especialista en informática, activista y fundadora de la Liga por la Justicia Algorítimica (Algorithmic Justice League) (Burton, 2020).

## 1. Entendiendo los sesgos y cómo explicarlos

En ese sentido, en primer lugar, el concepto de inteligencia artificial responsable no existía como tal hasta que, con el auge del *machine learning*, surge la demanda de comprensión sobre cómo funcionan los algoritmos y modelos e intentar que los responsables de estos sean capaces de rendir cuenta sobre su funcionamiento.

Lo cierto es que en muchas películas se reflejan muchos malos usos y consecuencias negativas de la IA, y existen casos reales de cajas negras, sistemas sesgados o desarrollos inesperados, en concreto por aquí mencionamos algunos:

– Cajas negras o sistemas de IA opacos que pueden «engañarnos». Por ejemplo, ante algunas aplicaciones, no somos capaces de distinguir que hay un sistema IA por debajo, y mucho menos se nos explica lo que hace o las decisiones que toma.
– Falsos positivos y discriminación fruto de sistemas sesgados. Fue el caso de un modelo para predecir la potencial reincidencia penal de una persona. El sistema estaba sesgado y penalizaba solo a personas negras.
– Desarrollos inesperados o negativos al poner en producción la inteligencia artificial. Está el ejemplo de un *chatbot* que aprendía de las interacciones en Twitter con los usuarios y que replicó malas palabras y conductas.

De hecho, estos sesgos pueden expandirse desde los datos a las decisiones del modelo. Un ejemplo de esto son los *word embeddings* generados con herramientas como GloVe, que se basan en textos de Wikipedia. Estos infieren el valor semántico de las palabras en función de las que aparecen alrededor. De hecho, el valor semántico de algunas profesiones estaba correlacionado con el valor semántico de *he* (él) o el de *she* (ella), existiendo un sesgo en los mismos *word embeddings* que luego se utilizarán para desarrollar herramientas y soluciones de procesamiento del lenguaje natural (PLN).

También suelen aparecer problemas de sesgos en sistemas de recomendación para la búsqueda de candidatos desde RR. HH. En otro ejemplo, una mujer con más experiencia y formación que un hombre estaba por debajo en el *ranking* resultante del modelo, cuando estas variables deberían ser las más determinantes.

## 2. Tipos y origen de los sesgos

Cuando hablamos de sesgos, podemos hablar de dos tipos. Por un lado, se puede producir una discriminación intencional o explícita (*disparate treatment*) y, por otro, una discriminación no intencional (*disparate impact*). Lo cierto es que los sistemas de inteligencia artificial normalmente reproducen esta última, pues los sesgos suelen ser fruto de un mal tratamiento de los datos con los que se ha entrenado el modelo.

Así pues, el origen de los sesgos puede darse en distintos pasos relacionados con los datos y variables de entrenamiento, como son:

1. La adquisición de los datos, que tienen un sesgo de por sí.

2. La definición o etiquetado de los datos, por error humano o criterios subjetivos.
3. El utilizar menos variables de las necesarias, por lo que se infieren relaciones erróneas entre los datos.
4. El desequilibrio de datos, que no son representativos y pueden discriminar a las minorías.

En este sentido, para trabajar con datos variables sensibles y abordar la problemática de los sesgos, hay que tener en cuenta el contexto legal. En muchas regulaciones ya se dice que variables como el sexo, la raza o la religión, entre otras, tienen que estar protegidas y no se puede discriminar por ellas.

En segundo lugar, la creciente adopción de IA en la toma de decisiones críticas ha generado preocupaciones sobre la equidad y la justicia. Uno de los principios que deberían guiar el desarrollo de la inteligencia artificial es el de *fairness* o justicia. Este pasa por asegurarnos de que las decisiones de nuestros algoritmos son justas y no se ven condicionadas por sesgos de raza o género, entre otros, y que normalmente vienen de los propios datos.

Por ejemplo, en la justicia penal, los algoritmos de predicción de reincidencia han mostrado sesgos raciales que pueden afectar negativamente a las personas de color (Ferrante, 2021, p. 33). De manera similar, en el ámbito de la salud, los sistemas de diagnóstico basados en IA pueden perpetuar desigualdades existentes si los datos de entrenamiento no representan adecuadamente a todas las poblaciones (Mullane, 2019). En cuestión de género, será importante trazar la estrategia más inteligente para que las nuevas identidades de género se admitan en las sociedades contemporáneas, incluso por sectores conservadores, sin que se reproduzcan las situaciones de agravio social que los colectivos LGTBIQ+ clásicos sufrieron durante décadas y siguen sufriendo en tantos países donde sus derechos no se ven aún reconocidos (Rivero Ortega, 2023, p. 14).

Este estudio se organiza de la siguiente manera: proporcionamos una revisión exhaustiva de la literatura sobre la definición conceptual de sesgos algorítmicos y sus causas. Luego describimos la metodología usando el enfoque cualitativo adoptado para analizar casos específicos de sesgos en IA. A continuación, se presentan los hallazgos principales, seguidos de un análisis detallado en la discusión ética y jurídica. Y finalmente, se ofrecen conclusiones y recomendaciones para futuras investigaciones y prácticas.

## Marco conceptual

El sesgo algorítmico se refiere a la predisposición sistemática que puede surgir en los modelos de IA debido a datos de entrenamiento sesgados o a su diseño. Según Hao (2019), el sesgo puede aparecer en diversas etapas del proceso de desarrollo del algoritmo, desde la definición del problema hasta la recolección y preparación de datos. Noble (2018, p. 138) destaca que los algoritmos pueden perpetuar y amplificar las desigualdades existentes si no se diseñan y monitorean adecuadamente. Barocas y Selbst (2016) argumentan que los sesgos

pueden entrar en los sistemas de IA a través de datos históricos que reflejan prejuicios humanos.

El sesgo en la IA puede tomar muchas formas, como el sesgo de selección, donde los datos de entrenamiento no representan adecuadamente a toda la población, o el sesgo de confirmación, donde los desarrolladores introducen involuntariamente sus propios prejuicios en los algoritmos. Según Diab, la reducción del sesgo de los datos es un desafío prioritario para que las normas funcionen efectivamente en el futuro del *machine learning* (Mullane, 2021). Este sesgo puede ser especialmente problemático en aplicaciones críticas, como en la justicia penal, donde los algoritmos de predicción de reincidencia han mostrado sesgos raciales significativos, afectando desproporcionadamente a personas de color (Ferrante, 2021).

## 1. Tipos de sesgos en IA

A) Sesgo de selección: este tipo de sesgo ocurre cuando los datos de entrenamiento no representan adecuadamente a toda la población. Por ejemplo, si un algoritmo de diagnóstico médico se entrena solo con datos de una población específica, puede no funcionar correctamente para otras poblaciones. Ferrante señala que uno de los problemas más comunes en el entrenamiento de modelos de IA es la falta de diversidad en los datos de entrenamiento, lo que puede llevar a resultados sesgados y poco representativos.

B) Sesgo de confirmación: este sesgo ocurre cuando los desarrolladores introducen involuntariamente sus propios prejuicios en los algoritmos. Esto puede suceder cuando se seleccionan variables que confirman las expectativas previas o cuando se ignoran datos que contradicen esas expectativas. Un ejemplo notable es el caso de los algoritmos de selección de personal que prefieren a candidatos masculinos debido a la prevalencia histórica de hombres en ciertos roles.

C) Sesgo de exclusión: se refiere a la omisión de variables importantes que pueden influir en el resultado del modelo. Por ejemplo, no incluir datos socioeconómicos relevantes en un modelo de crédito puede llevar a decisiones injustas que perjudican a ciertos grupos demográficos.

D) Sesgo de agrupación: ocurre cuando los algoritmos agrupan datos de manera que refuerzan estereotipos o simplifican en exceso las características de ciertos grupos. Esto puede ser particularmente problemático en aplicaciones de reconocimiento facial, donde los algoritmos pueden tener dificultades para distinguir entre individuos de grupos minoritarios (Ferrante, 2021).

## 2. ¿Cómo evitar los sesgos en la inteligencia artificial?

La primera decisión que se suele tomar para desarrollar una Inteligencia Artificial sin sesgos es evitar las variables sensibles. No obstante, estas pueden estar correlacionadas con otras que sí se utilicen y que reproducen los mismos sesgos indirectamente. Por ello, surgen distintas métricas de *fairness* para saber si se puede estar discriminando a un colectivo.

Para entenderlas, existe el ejemplo de un modelo que decide a quién darle un crédito y que podía tener un sesgo de género, medible mediante:

a) Criterios de independencia, que comprueban que la predicción del modelo condicionado a la variable de género no tenga valores muy dispares. No son infalibles, porque no tienen en cuenta cierta información.
b) Criterios de separación, para que la proporción de predicciones del modelo sea similar, no solamente condicionada a que la persona sea hombre o mujer, sino también condicionada a si ha devuelto el crédito o no.
c) Criterios de suficiencia, para que la proporción de personas que han devuelto en crédito sea similar en el caso de hombres y en el de mujeres.

Esas métricas de *fairness* se pueden aplicar en distintos puntos del proceso de desarrollo de un modelo: al analizar datos de entrada, para corregir un posible desequilibrio, durante el entrenamiento del modelo *per se*, o si el modelo ya está desplegado, hay técnicas de *fairness* para corregir el sesgo.

## 3. Consecuencias del sesgo algorítmico

Las consecuencias del sesgo algorítmico pueden ser graves y variadas. En el ámbito de la justicia penal, por ejemplo, los sesgos pueden llevar a decisiones injustas que afectan desproporcionadamente a ciertos grupos raciales o étnicos. En la salud, los sesgos en los algoritmos de diagnóstico pueden resultar en tratamientos inadecuados para ciertos pacientes. Además, en el ámbito laboral, los sesgos en los sistemas de selección de personal pueden perpetuar desigualdades de género y raza (Noble, 2018, p. 139).

Según un estudio de Buolamwini y Gebru (2018), los sistemas de reconocimiento facial tienen tasas de error significativamente más altas para mujeres y personas de color en comparación con hombres blancos, lo que evidencia un sesgo sistemático en la tecnología de visión artificial. Este tipo de sesgo no solo perpetúa las desigualdades existentes, sino que también puede amplificarlas, afectando negativamente a las personas que ya están en desventaja.

Ahora también suscita numerosas dudas la policía preventiva, que emplea algoritmos para anticipar el crimen y evitar reincidencias. La utilización de la biometría es otro de los asuntos más controvertidos, por su potencial vulneración de derechos fundamentales. En los últimos años, tanto a nivel de tecnología como a nivel de casos de uso, incluso dentro de la regulación, en el caso del RGPD tiene artículos en los que se dice explícitamente que es deseable que cuando un sistema de IA tome decisiones sensibles dé explicaciones.

## Análisis con enfoque cualitativo

Este estudio utiliza un enfoque cualitativo, basado en la revisión de literatura y análisis de casos prácticos. Se examinan estudios previos sobre sesgos en IA y se analizan casos documentados de sesgos en aplicaciones de IA en diferentes sectores, como el reconocimiento facial y la selección de personal.

La revisión de literatura incluye la selección de artículos académicos, informes técnicos y documentos de organizaciones relevantes en el campo de la IA. Se utilizaron bases de datos académicas como Google Scholar, PubMed y JSTOR para identificar fuentes relevantes. Los criterios de inclusión fueron estudios que abordaran el sesgo algorítmico, sus causas, efectos y posibles soluciones.

El análisis de casos prácticos se centró en ejemplos documentados de sesgos algorítmicos en aplicaciones críticas. Se seleccionaron casos en sectores como la salud, la justicia penal y el empleo. Cada caso se analizó en términos de cómo surgieron los sesgos, sus impactos y las medidas adoptadas para mitigarlos.

## Principales resultados

Los resultados del análisis de casos muestran que los sesgos algorítmicos pueden manifestarse de diversas formas y tener impactos significativos en las decisiones basadas en IA. Por ejemplo, se ha encontrado que los sistemas de reconocimiento facial tienen tasas de error más altas para personas de color en comparación con personas blancas. En la selección de personal de Amazon, los algoritmos han mostrado preferencia por candidatos masculinos debido a la prevalencia de datos históricos sesgados hacia hombres en ciertos roles. Las entrevistas con expertos resaltaron la necesidad de una mayor transparencia y responsabilidad en el diseño de sistemas de IA (Ferrante, 2021).

*Caso 1: reconocimiento facial*

Un estudio de Buolamwini y Gebru reveló que los sistemas comerciales de reconocimiento facial desarrollados por empresas como Amazon, IBM y Microsoft funcionaban mejor con rostros de personas blancas que con rostros de personas negras. Este sesgo se debe en parte a la falta de diversidad en los datos de entrenamiento utilizados para desarrollar estos sistemas. La investigadora Joy Buolamwini destacó que los algoritmos de reconocimiento facial a menudo no reconocen correctamente los rostros de personas negras, lo que puede tener graves implicaciones en aplicaciones de vigilancia y seguridad.

*Caso 2: selección de personal*

En 2018 se descubrió que un algoritmo de selección de personal desarrollado por Amazon mostraba una clara preferencia por candidatos masculinos. Este sesgo se originó porque el algoritmo fue entrenado con datos históricos de solicitudes de empleo, la mayoría de los cuales provenían de hombres. Como resultado, el sistema penalizaba las solicitudes que contenían palabras clave relacionadas con actividades femeninas, como «equipo de mujeres». Este ejemplo ilustra cómo los datos históricos pueden perpetuar y amplificar las desigualdades existentes.

*Caso 3: diagnóstico médico*

En el ámbito de la salud, un estudio encontró que un algoritmo utilizado para predecir el riesgo de enfermedades crónicas subestimaba sistemáticamente el riesgo para los pacientes negros en comparación con los pacientes blancos (Ferrante, 2021). Este sesgo se debió a que el algoritmo utilizaba datos de costos de

atención médica como un *proxy* para la salud, y los pacientes negros, que tienden a tener menos acceso a la atención médica, aparecían como menos enfermos en los datos.

Varias aplicaciones y programas han sido cuestionadas por juristas y tribunales. Así, Compas, en Estados Unidos, por sus efectos de discriminación racial, o Syri, en Europa, por su incidencia sobre las garantías clásicas, son dos de ellos.

El programa Compas ha sido particularmente controvertido, hasta el punto de protagonizar la crítica en artículos relevantes de las principales revistas jurídicas de los Estados Unidos. También la opinión pública ha conocido esta polémica, a través de medios tan célebres y prestigiosos como el New York Times. El hecho es que los jueces norteamericanos se basaron en sus resultados para decidir el ingreso en prisión de personas por el riesgo de reincidencia, hasta el cuestionamiento jurisprudencial de un posible sesgo.

## 1. Discusión

Los hallazgos indican que los sesgos algorítmicos son un problema prevalente y significativo. Comparando con la literatura existente, este estudio confirma que la presencia de sesgos puede tener consecuencias graves, como la discriminación y la perpetuación de desigualdades sociales (Mullane, 2021). Para mitigar estos efectos, se recomienda implementar prácticas de desarrollo más inclusivas y realizar auditorías regulares de los sistemas de IA. Además, es crucial promover la educación y la conciencia sobre los sesgos entre los desarrolladores y los usuarios de IA.

La investigación de Ferrante (2021) sugiere que la diversidad en los equipos de desarrollo es esencial para detectar y corregir los sesgos algorítmicos, ya que los desarrolladores aportan sus propias visiones del mundo y prejuicios al diseño de los sistemas. Esto subraya la importancia de incluir a personas de diversos antecedentes y experiencias en el proceso de desarrollo de IA para garantizar que los sistemas sean justos y equitativos (Carrero Herrera, 2023).

Pero… ¿debemos renunciar a los algoritmos? Esta pregunta no puede responderse negativamente porque, de hecho, ninguna organización en contexto competitivo (incluidos, por supuesto, los Estados) se puede permitir no aprovechar las ventajas y beneficios que ofrece en nuestro tiempo la inteligencia artificial.

Toda la crítica observada sobre los sesgos de los algoritmos puede calificarse como un efecto reverso de una gran transformación tecnológica y social, no calibrada ni anticipada por los promotores del empleo creciente y exitoso de la inteligencia artificial.

En realidad, se nos dice por autores diversos, que los sesgos también son propios de las decisiones humanas, contaminadas así mismo por el «ruido», un elemento ajeno a los algoritmos, lo que les da una ventaja para no cometer errores. Además, «la posibilidad de corregir los prejuicios del programador mediante modulaciones del algoritmo debe tenerse muy en cuenta, porque no es tan

sencillo corregir las tendencias discriminatorias de mujeres y hombres» (Sunstein, 2022, p. 1189).

## 2. Implicaciones éticas y sociales

El sesgo algorítmico plantea importantes desafíos éticos y sociales. La automatización de decisiones críticas a través de la IA puede exacerbar las desigualdades existentes y crear nuevas formas de discriminación. Es fundamental que los desarrolladores de IA consideren las implicaciones éticas de sus tecnologías y trabajen para mitigar los sesgos que pueden surgir. Ferrante argumenta que la equidad algorítmica debe ser una prioridad en el desarrollo de IA, y que las decisiones automatizadas deben ser transparentes y responsables. Esto implica no solo el desarrollo de tecnologías justas, sino también la creación de marcos regulatorios y políticas que garanticen el uso ético de la IA (Asquerino Lamparero, 2021, p. 357).

La falta de ética de los programas informáticos es el punto de discusión. Tecnólogos como Kerns y Roth se han propuesto generar algoritmos éticos, introduciendo prevenciones frente a su orientación «antisocial», para evitar los sesgos, pero son muchos los problemas que plantea la protección de la privacidad (por las dificultades prácticas de la anonimización de datos de forma plena, dado el nivel de intromisión de los dispositivos en nuestra privacidad) y la casi imposible compatibilidad de la corrección plena y el nivel deseado de precisión de las herramientas.

También señalan diversos autores las diferencias culturales que pueden suscitarse en el debate sobre las minorías o colectivos a proteger, los criterios a utilizar y las ponderaciones concretas. Para varios de ellos, el problema es la raza, otros se centran en el género y por supuesto la edad se convertirá antes o después en un dato diferencial de riesgo discriminatorio (Cotino Hueso y Bauzá Reilly, 2022).

## 3. Estrategias para mitigar el sesgo algorítmico

1. Diversificación de datos de entrenamiento: asegurarse de que los datos utilizados para entrenar los modelos de IA sean diversos y representativos de la población general es fundamental. Esto puede incluir la recopilación de datos de múltiples fuentes y la inclusión de variables demográficas importantes para evitar la exclusión de grupos específicos.
2. Auditorías algorítmicas: realizar auditorías regulares de los algoritmos para detectar y corregir sesgos. Estas auditorías deben incluir pruebas de rendimiento en diferentes subgrupos demográficos y el análisis de decisiones algorítmicas para identificar patrones de discriminación.
3. Transparencia y explicabilidad: promover la transparencia en el desarrollo y uso de algoritmos de IA. Los desarrolladores deben ser capaces de explicar cómo funcionan sus algoritmos y cómo se toman las decisiones. Esto incluye la documentación detallada de los datos utilizados, los procesos de entrenamiento y las métricas de rendimiento.

4. Educación y capacitación: fomentar la educación y la capacitación en ética de IA entre los desarrolladores y usuarios. Esto puede incluir cursos y talleres sobre equidad algorítmica, así como la inclusión de estos temas en los programas de formación de ciencias de la computación.
5. Enfoques interdisciplinarios: colaborar con expertos de diferentes disciplinas, como la sociología, la psicología y el derecho, para desarrollar enfoques más holísticos para la detección y corrección de sesgos. La integración de perspectivas diversas puede ayudar a identificar y abordar problemas que pueden no ser evidentes desde una única disciplina (Mullane, 2021).

En algún punto, afirman, debe producirse el acuerdo entre los tecnólogos y los reguladores, para alcanzar ese equilibrio entre precisión y corrección, porque la desaparición de ciertos criterios selectivos podría afectar al grado de exactitud de la decisión, afectando los objetivos mismos de la política pública. Y, en algunos casos, consideran directamente que los algoritmos no deberían tomar ciertas decisiones (ponen el ejemplo del vehículo no tripulado que se programa para sacrificar una vida en el intento de salvar varias). En ese sentido, lo cierto es que «algunas decisiones no deberían depender de las máquinas, ni desvincularse de la moralidad humana» (Sandel, 2016).

Estamos ante principios de un nuevo realismo jurídico, ¿sí o no?

La excelente tradición jurídica evidencia su contribución al progreso civilizatorio, la mejor versión de la cultura de nuestras sociedades. Si todo el desarrollo humano debe interpretarse en clave de ampliación de capacidades, las posibilidades abiertas por los cambios normativos y las interpretaciones jurisprudenciales son considerables: la ampliación de las libertades y los derechos, el reconocimiento de la equidad en las relaciones económicas, la protección de los sectores más vulnerables. Todas estas son aportaciones del derecho para realizar un concepto universal de justicia.

Ejemplos sobran: el matrimonio, por ejemplo, se ha preconcebido para albergar relaciones afectivas entre personas del mismo sexo. La función pública ha de respetar hoy la igualdad de género. Poco a poco, todo el avance tecnológico se incorpora a marcos regulatorios que no bloquearon su despliegue, y previenen riesgos derivados de la incertidumbre y de la perplejidad del Estado.

Si los algoritmos son injustos, deben corregirse sus prejuicios, que son los de las personas o instituciones que los diseñaron. Cualquier resistencia extrema a los progresos sociales o tecnológicos carece del requisito de la razonabilidad, no es sensata.

La proporcionalidad evoca una idea de adecuación entre medios y fines que podrían ser apropiados al pronunciarse sobre la aceptabilidad del uso de herramientas de inteligencia artificial, incluyendo los algoritmos. Al mismo tiempo, el principio de progresividad, en cambio, aboga por la incorporación de estas herramientas a la gestión de los servicios públicos, incluso desde el punto de vista del principio o derecho a la buena administración, toda vez que los algoritmos, «pueden incrementar el grado de objetividad de las decisiones, y su motivación

puede ser más previsible si los programas que utilizan se hacen públicos, como la doctrina viene exigiendo»[2].

## Conclusiones

Con este artículo hemos explorado los sesgos algorítmicos en la IA, destacando sus causas, efectos y posibles soluciones. Se concluye que la identificación y mitigación de los sesgos es esencial para asegurar que la IA se utilice de manera justa y equitativa. Las recomendaciones incluyen mejorar la calidad y diversidad de los datos de entrenamiento, aumentar la transparencia en el desarrollo de algoritmos y fomentar una cultura de responsabilidad entre los desarrolladores de IA. Futuros estudios podrían centrarse en desarrollar metodologías específicas para la detección y corrección de sesgos en diversas aplicaciones de IA.

La inteligencia artificial responsable tiene que seguir desarrollándose. Sobre todo, para que se aplique a todo tipo de modelos, incluso los que puedan surgir, y que estos nos den cada vez mejores explicaciones.

Además, es crucial que los desarrolladores y usuarios de IA estén conscientes de los sesgos potenciales y trabajen activamente para mitigarlos. Esto requiere un enfoque multidisciplinario que incluya no solo a ingenieros y científicos de datos, sino también a expertos en ética, derecho y ciencias sociales. Solo a través de un esfuerzo concertado y colaborativo se pueden abordar adecuadamente los desafíos del sesgo algorítmico y garantizar que la IA beneficie a todos los miembros de la sociedad.

Finalmente, nos preguntamos: ¿puede hoy el derecho propiciar tal cambio? Lo que las normas y principios jurídicos sí han de propiciar es la garantía del respeto de todas las personas, de su dignidad, libertad y derecho a ser tratados por los demás conforme al autorreconocimiento de su identidad.

Es positivo asumir la ventaja tecnológica porque los algoritmos pueden alcanzar un grado de precisión y automatismo en la aplicación de criterios objetivos al que hemos aspirado como remedio a las corruptelas y preferencias subjetivas de las personas. Pero también, procede garantizar la protección de la dignidad de la persona, la anonimización de sus datos y su autodeterminación, cuando los algoritmos la afectan.

Si los movimientos de transformación tecnológica o social intentan imponerse sin atención a los efectos que ocasionan sobre las percepciones y los intereses de las personas generarán reacciones adversas. Y el papel del derecho, en su versión de ciencia jurídica responsable, es buscar y propiciar los equilibrios y aceptaciones de los distintos puntos de vista, facilitando la convivencia.

2 Sobre la publicidad de los algoritmos, revisar a Boix Palop (2022).

## Referencias bibliográficas


Asquerino Lamparero, M. J. (2021). *Algoritmos y discriminación*. Universidad de Sevilla.

Barocas, S., Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review, 104*(3), 671-732.

Boix Palop, A. (2022). Transparencia en la utilización de la inteligencia artificial por parte de la Administración. *El Cronista del Estado Social y Democrático de Derecho*, (100).

Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81, 1-15.*

Burton, S. (Dir.). (2020). *Coded Bias* [Película]. 7th Empire Media. Disponible en Netflix.

Carrero Herrera, J. M. (2023). Sesgo algorítmico en la Inteligencia Artificial: Abordando la toma de decisiones erróneas. *LinkedIn*. https://www.linkedin.com/pulse/sesgo-algor%C3%ADtmico-en-la-inteligencia-artificial-toma-carrero-herrera/

Cotino Hueso, L., Bauzá Reilly, M. (2022). *Derechos y Garantías ante la Inteligencia Artificial y las Decisiones Automatizadas*. Thomson Reuters Aranzadi.

Ferrante, E. (2021). Inteligencia artificial y sesgos algorítmicos: ¿Por qué deberían importarnos? *Nueva Sociedad, 294,* 28-36.

Hao, K. (2019). Cómo se produce el sesgo algorítmico y por qué es tan difícil detenerlo. *MIT Technology Review*. https://www.technologyreview.es/s/10924/como-se-produce-el-sesgo-algoritmico-y- por-que-es-tan-dificil-detenerlo

Mullane, M. (2021). La eliminación de los sesgos en los algoritmos. *Revista UNE,* (11), 1-5.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Rivero Ortega, R. (2023), Algoritmos, sesgos, sexos y géneros: la sensatez del Derecho. *Revista de la Facultad de Derecho de México*, *73*(285).

Sandel, M. (2016). *What Money can't buy. The Moral limits of Markets*. Penguin. https://scholar.harvard.edu/sandel/publications/what-money-cant-buy-moral-limits-markets

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 123-135

# LA INTELIGENCIA ARTIFICIAL Y LOS DERECHOS HUMANOS

*ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS*

**Cyntia Raquel Rudas Murga**

Directora del Instituto Peruano de Investigación Jurídica y Cibernética.
Docente en la Universidad Nacional Mayor de San Marcos.

## Resumen

En el presente siglo, el equilibrio jurídico entre la innovación tecnológica y la protección de los derechos humanos es un desafío constante. En el la presente investigación se busca determinar *prima facie* el impacto de la inteligencia artificial (IA) en los derechos humanos, utilizando el experismo y la descripción de hechos. La IA ha experimentado un crecimiento exponencial en las últimas décadas, revolucionando múltiples aspectos de la vida cotidiana. Desde los asistentes virtuales pasando por el internet de las cosas y el uso de IA en la resolución judicial de casos.

La IA tiene un impacto positivo y negativo sobre los derechos humanos. En el marco universal las Naciones Unidas, el Consejo de Europa, la UE, la OEA entre otras organizaciones internacionales en derechos humanos están reflexionando y tomando medidas ante estos retos tecnológicos. Sin embargo, este avance tecnológico plantea importantes cuestiones éticas y jurídicas, particularmente en derechos humanos. La educación y la concientización pública son decisivos para empoderar a las personas en el uso de la IA y así garantizar la protección de sus derechos humanos.



## Palabras clave

IA, derechos humanos, ética, conciencia digital, constitucionalismo digital.



## Abstract

In this century, the legal balance between technological innovation and the protection of human rights is a constant challenge. This research seeks to determine in prima facie the impact of artificial intelligence (AI) on human rights, using experientialism and facts description. AI has experienced an exponential growth in recent decades, revolutionizing multiple aspects of daily life, from virtual assistants to the internet of things and the use of AI in the judicial resolution of cases.

AI has a positive and negative impact on human rights. In the universal framework, the United Nations, the Council of Europe, the EU, the OAS, among other international human rights organizations, are reflecting and taking measures to address these technological challenges. However, this technological advance raises important ethical and legal questions, particularly in human rights. Education and public awareness are critical to empowering people in the use of AI and thus ensuring the protection of their human rights.



## Keywords

AI, human rights, ethics, digital awareness, digital constitutionalism.

## *Building a Digital Culture*

### Contexto

El equilibrio entre la innovación tecnológica y la protección de los derechos humanos es un desafío constante, pero es un desafío que se debe afrontar de manera colectiva a fin de construir un futuro más justo y equitativo. La injusticia en cualquier parte es una amenaza a la justicia en todas partes, Martín Luther King lo identificaba en los setenta, porque son características jurídicas propias de la dignidad y la vida como parte de una infraestructura constitucional garante de los derechos humanos superando la teoría de un Estado de Derecho y ampliado a un Estado Constitucional de Derecho con un alcance al Estado de los derechos humanos digitales emergentes.

En este contexto, el uso indebido de la IA impacta de forma negativa a los derechos humanos, puede afectar a la vida, la dignidad, la intimidad, la no discriminación, la igualdad, privacidad, salud, el trabajo, la libertad de expresión, libertad de reunión, identidad personal, educación, al juicio justo, la tutela jurisdiccional efectiva digital, a los derechos de los pueblos indígenas, a los derechos de autor, propiedad intelectual, entre otros. Sin embargo, el uso idóneo, debido, razonable y normado de la IA por su naturaleza y condición coadyuva de manera transversal en la solución de problemas globales y seculares de la sociedad pero también plantea relevantes desafíos para los derechos humanos.

### Marco legal

La Declaración Universal de los Derechos Humanos (DUDH) de 1948 reconoce el derecho a la privacidad y la no discriminación. Asimismo, conforme con el *soft law*, la OCDE estableció las Directrices sobre Inteligencia Artificial en el 2019 para promover la IA ética y segura, con énfasis en la transparencia, la responsabilidad y la gobernanza. Por su parte, la Asamblea General de la ONU, a través de sus resoluciones, aborda la IA y sus implicaciones, incluida la necesidad de proteger los derechos humanos en su desarrollo y uso.

La Unión Europea cuenta con el Reglamento General de Protección de Datos (GDPR-2018) que establece normas estrictas para la protección de datos personales, incluidos los datos utilizados en aplicaciones de IA.

En Estados Unidos, precisamente en el estado de Illinois, a consecuencia de que *Pay By Touch*, una *startup*, se declaró en quiebra y se esperaba que subastaran sus activos incluida su base de datos sensibles de sus usuarios (huellas digitales), el Legislativo en el 2008 emite la Ley de Privacidad de la Información Biométrica, con la finalidad de exigir a las empresas que obtengan el consentimiento antes de recopilar la información biométrica, y crear una política sobre la administración y destrucción de la data.

Asimismo, en Perú se tiene vigente la Ley 31.814 del 5 de julio de 2023, que promueve el uso de la IA en favor del desarrollo económico y social del país. El objeto de la ley es promover el uso de la IA en el marco del proceso nacional de transformación digital privilegiando a la persona y el respeto de los derechos

humanos con el fin de fomentar el desarrollo económico y social del país en un entorno seguro que garantice el uso ético, sostenible, transparente, replicable y responsable; esta Ley si bien es mejorable se considera la existencia de un paso a la regulación nacional sustentada en la constitucionalidad digital fundante en un Estado Social de Derecho.

Es así que en el ordenamiento jurídico peruano, uno de los temas que se adiciona al estudio de la IA y los derechos humanos son los datos personales contenidos en la Ley de Protección de Datos Personales (LPDP), Ley 29.733 de 2011 y su reglamento, previsto de similar manera en la Constitución Política del Perú de 1993, en el artículo 2, numeral 6: «A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar». Noción que debe analizarse de forma extensiva con el uso de la IA.

## Evolución de la inteligencia artificial

Las innovaciones tecnológicas han evolucionado de forma transversal e interdisciplinaria más aún con la puesta en marcha la IA como un instrumento de análisis y procesamiento de *data, big data* o *metadata*, obteniendo un resultado en milésimas de segundos superando la capacidad humana. Sin embargo, el uso desproporcionado e irrazonable de la IA podría acarrear irreparables consecuencias puesto que existen espacios aún no desarrollados científicamente cómo determinar con precisión el impacto en el buen aprendizaje —como la evolución del aprendizaje tradicional, el aprendizaje automático (telemático, disposición de tiempo, elección *topic*, asistencia de ChatGPT)— y la vulneración de los derechos humanos en la construcción de una gobernanza y la constitucionalización digital.

Algunos derechos analizados desde el enfoque de la IA son la intimidad, la privacidad, la libertad de expresión, la igualdad y la discriminación racial. Otra de nuestras preocupaciones son los espacios o medios tecnológicos tangibles o intangibles que deben ser seguros para el ejercicio propio de la garantía de los DD. HH. y que no pudieran verse afectados por la inseguridad de red; entendiendo a la seguridad de red como el conjunto de estrategias, procesos y tecnologías diseñados para proteger determinada red frente a terceros.

En este sentido, estudiar a la inseguridad en red implica también analizar la ciberseguridad, puesto que la ciberseguridad en Corea (2022) se incrementó debido al ataque cibernético que permitió por ejemplo, la fuga de los códigos fuentes, la manufactura desmesurada de celulares, la negación de servicios por ataques. En este sentido, Katherina Canales (2023) sostuvo que «América Latina es un blanco» y que «llegamos 10 años tarde a la discusión [sobre ciberseguridad] y a la fecha no existe una política nacional de ciberseguridad».

En este contexto evolutivo de la IA, la ciberseguridad puede ser entendida como la práctica operativa y teórica de proteger equipos, redes, aplicaciones de *software*, sistemas críticos y datos ante posibles amenazas digitales. Algunos tipos de ataque son: *malware, ransomware,* ataque de intermediario, *DDoS,*

amenaza interna, además de la participación relevante de la persona, se describen algunas conductas que ocupan especial interés al derecho, como son: *black hat*, *grey hat*, *white hat* o *hackers*, *newbies*, *hacktivista*, *phreakers*, *hackers* de ingeniería social, *hackers* de *hardware* y *hackers* de redes.

Por lo tanto, la ciberseguridad es un asunto de Estado y no solo de gobierno, de empresas, que también compromete a las entidades públicas y privadas pero sobre todo a los ciudadanos, quienes tienen la capacidad de cuidar su información y sus datos personales. La pregunta es: ¿quién o quienes cuidarán de la información de los niños y niñas así como de los analfabetos digitales? ¿Se encuentran expuestos sus derechos humanos con el uso de la IA asociada o como consumidores de programas con IA?

Para ello, no solo es necesario tener «puntos focales normativos de conexión» a fin de lograr regulaciones específicas e identificar los delitos cibernéticos, así como revisar los compromisos de las empresas prestadoras o facilitadoras de la *app* o del servicio a fin de garantizar el cuidado y respeto a los derechos humanos y construir una cultura digital.

Es así que en esta evolución tecnológica, la IA *per se* no cuenta con una definición propia o un concepto claramente definido; sin embargo, la IA tiende a ser un *machine learning,* una máquina con capacidad de aprender, imitar, crear, entender, con cierta sensibilidad desarrollada, uso de un lenguaje y capacidad para la percepción del ambiente. Para su estudio la subdividimos en inteligencia artificial predictiva (IAP) e inteligencia artificial generativa (IAG).

En primer lugar, la IAP para este estudio se considera como una rama de la IA y un método de análisis de datos que permite predecir y anticipar necesidades o eventos futuros basados en una casuística pasada, analizando datos históricos y patrones. Es una tecnología que puede simular un conjunto de escenarios para alinear la estrategia de la empresa, compañía o a nivel jurisprudencial a modo de plenos casatorios, puede predecir un tipo de resultado muy asertivo a la solución posible del caso jurídico propuesto, teniendo presente las causas y consecuencias del tipo de sesgo.

En segundo lugar, la IAG es una rama de la IA que se enfoca en la generación de contenido original a partir de datos existentes y programados. Es una tecnología que utiliza algoritmos y redes neuronales avanzadas para desarrollarse por sí misma, aprender textos y desarrollar imágenes para después generar un contenido nuevo e irrepetible. En definitiva, «la IA tiene la capacidad de imitar funciones cognitivas de la mente humana, como: la creatividad, sensibilidad, aprendizaje, entendimiento, percepción del ambiente y uso del lenguaje» (Grigore, 2022). Entonces, la IA es una herramienta poderosa en la toma de decisiones y la automatización del *big data* o *metadata*. En el ámbito legal la IA cobra mejor participación en el procesamiento de información, revisión de documentos legales y aceleración de los procesos judiciales desprendiendo algunos beneficios como el desahogo procesal, la obtención de un diagnóstico legal con opinión previa, la inmediatez procesal, la uniformidad de criterios en las jurisprudencias, la tranparencia en las resoluciones judiciales y lograr la eficacia en el acceso a la justicia.

## Derechos humanos

Sobre los derechos humanos, realizaremos una breve descripción hitórico-legal con la finalidad de contextualizar el uso de la IA en el plano jurídico. La Comisión Interamericana de los Derechos Humanos (CIDH), como órgano principal y autónomo de la Organización de los Estados Americanos (OEA), está encargada de la promoción y protección de los DD. HH. en el continente americano. A su vez, la Corte IDH, que integra el Sistema Interamericano de Protección de los Derechos Humanos (SIDH) desde 1979, resuelve asuntos propios en DD. HH. y posiblemente en un tiempo corto resuelva asuntos de disputa con el uso de la IA. Con la aprobación de la Convención Americana sobre los Derechos Humanos (CADH) constituida en 1969 y vigente a partir de 1978, se garantizan los derechos y las libertades de las personas; además de comprometer a los Estados miembro en adoptar las disposiciones jurídicas, políticas y administrativas necesarias en sendos ordenamientos jurídicos: «Artículo 1. Los Estados partes en esta Convención se comprometen a respetar los derechos y libertades (...)» y el Artículo 2: Deber de adoptar disposiciones de derecho interno, que a la letra señala:

> Si en el ejercicio de los derechos y libertades mencionados en el artículo 1° no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados partes se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta Convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades

En este contexto, cada país está obligado en adoptar las medidas necesarias para garantizar los derechos y libertades conforme a esta Convención y tomar las decisiones que fueren necesarios para efectivizar dicha protección. Asimismo, es indispensable que el Poder Ejecutivo, Legislativo y Judicial promuevan, desarrollen y ejecuten políticas favorables que aseguren las Garantías Judiciales y la Protección Judicial en cada Estado conforme sus competencias, concordante con los artículos 8 y 25 de la CADH.

Asimismo, en el segundo informe sobre la Situación de los Derechos Humanos en el Perú, la CIDH (2000) analiza el impacto y la influencia en los DD.HH., describiendo una dura y crítica realidad de afectación a los mismos, explicados en diversos estados de estudio.

La CIDH es un órgano principal de la OEA que tiene el propósito de promover la observancia y defensa de los derechos humanos y actuar como órgano de consulta de la Organización. En consecuencia, la CIDH ha utilizado diversos mecanismos y prácticas en el ejercicio de sus funciones y en el cumplimiento de sus mandatos, incluyendo visitas *in loco*, redacción de informes generales y especiales, tramitación de casos individuales y organización de actividades de promoción de los derechos humanos. (CIDH, 2000, Párr. 1)

De esta manera la CIDH puede realizar visitas *in loco* en Perú, así como en los treinta y cuatro Estados miembros firmantes, a fin de dar cabal cumplimiento a la CADH, situación que implica analizar las diversas posibilidad de tratamiento juridico y resolucion de conflictos entre los DD. HH. y el uso de la IA.

Por su parte, el derecho constitucional según su innata naturaleza emerge para garantizar la protección de los derechos fundamentales, asegurar las libertades, aplicar la tutela jurisdiccional efectiva, y la garantía procesal constitucional es así que teniendo las bases normativas sobre derecho humanso es sumamente más accesible que cada país adecue el uso de la IA en su ordenamiento jurídico y de esta manera se desarrolle una gobernanza digital en IA integrada y consolidada de forma intercontinental antropocentrista.

Bajo esta descripción, la constitucionalización digital implica una articulación entre operadores de justicia, abogados, sociedad cibernética, sociedad civil y ciudadanía de forma holística porque aquello implicaría desarrollar nuestra conducta en armonía con la filosofía del Estado Constitucional de Derecho, la justicia y el uso idóneo de la IA. Es por ello que se pretende verter una serie de ideas, reflexiones y críticas que han desarrollado el tema relativo a la constitucionalización digital, para luego de la confrontación de ideas doctrinales, obtener una conclusión que permita afirmar cuál «debe ser» la forma de interpretar y aplicar el derecho digital en los tiempos actuales, teniendo como centro a la Constitución dentro del ordenamiento jurídico como que fuente de fuentes del derecho contemporáneo así como los derechos del siglo XXI.

En este sentido, las innovaciones tecnologías con el uso de IA también son mecanismos que facilitan e inmediatizan el acceso a la justicia por ejemplo, los *straps app law*, jurisprudencia y la doctrina que implica la posibilidad de procesar miles de documentos para aportar al proceso —necesario en la etapa del intercambio de documentos o presentación de medios de prueba— incluido el diagnóstico, utilizado sobre todo en procesos de arbitraje, pero aplicables a determinados proceso judiciales. Otra de las utilidades de la IA en la justicia son las *apps* de seguimiento de una persona detenida hasta la reinserción social, el cómo y el procedimiento serían los objetos para un eficaz seguimiento y de esta manera permita obtener un resultado esperado con impacto social.

En este contexto jurídico, la IA analiza toda la normativa posiblemente brindada a través de la programación y con la IAG la información que pueda generar, la doctrina, bases teóricas, jurisprudencia y el cotejo entre los resultados de otros casos similares, procesa y rastrea más de diez mil sentencias o fuentes por segundo se diferencia de un buscador convencional porque no responde con un listado de información, sino la respuesta más acertada para el caso. Así, se tiene a la *startup* canadiense Ross, del ordenador Watson de IBM, este sistema de «*machine learning* evoluciona como un *deep learning,* tecnología de IAP e IAG en cuanto más casos resuelve más aprende, en cuanto más interactúa con los seres humanos perfila su respuesta»; esta tecnología sitúa la incertidumbre del futuro de la abogacía, el reemplazo de ciertas actividades de los asistentes junior y senior así como, los trabajos mecánicos que se realizan en la estructura judicial, firmas de abogados y abogados litigantes.

Una de las discusiones temáticas versa en la posibilidad de que la IA emita sentencias. A pesar de la existencia de simuladores de la sentencia, algoritmos basados en casuística similar precedente y resuelve sin la posibilidad de la discrecionalidad razonada a fin de evitar contaminar la decisión por sesgos existentes en casos anteriores o por prejuicios casuísticos, en este caso se habla de la

«potencialidad dañosa de la IA en las decisiones judiciales». Es por ello, que el juez sigue tomando la última decisión sin negar que también conserva su propio sesgo humano.

En la actualidad, varios países utilizan la IA para resolver asuntos judiciales, en Estados Unidos el sistema Compas (*Correctional Offender Management Profiling for Alternative Sanctions*) a nivel penal —como uno de los programas pioneros— integra el cuestionario algorítmicamente para determinar su internamiento o excarcelación, se trata de la decisión sobre la libertad de tránsito con una PPL, decisión trascendente, considerándose factible auditar el algoritmo.

En China, por ejemplo, la experiencia es más avanzada, puesto que el tribunal de internet está conectado con los órganos del Estado (sistematización de la nación, cruce de datos). Aquí las decisiones se dictan utilizando IA. Sin embargo, el juez puede apartarse de dicha recomendación, pero debe fundamentar bajo cargo y responsabilidad. Esta estructura interconectada con diversas entidades del Estado limita a una persona condenada que incumple con la sanción por ejemplo a comprar un pasaje, ingresar a determinados lugares, etc.

Así como este caso, se tiene al juez holográfico con una telepresencia tridimensional con sensaciones parecidas a las humanas en la realidad virtual y aumentada con máscaras, lentes y sensaciones, hacia allá vamos y es posible que no haya retorno.

En efecto, los cibernautas o usuarios de la red por su condición y naturaleza humana se integran al amparo del derecho constitucional, puesto que los derechos fundamentales no se subrogan, ni extinguen, ni son permisibles de una recategorización, sino por el contrario los hechos jurídicos (fenómeno jurídico, conducta procesal) se mantienen sobre su misma tipificación tradicional modificando el uso de las tecnologías, el uso de la herramienta tecnológica y la IA.

## La IA en la vida de los servicios públicos y privados

Es por ello que después de la covid-19, la *googlización* (Rudas, 2017) y el internet de las cosas quedan superadas y se ubica un nuevo estándar teórico a resolver el «constitucionalismo en la era digital». Las redes sociales y los aplicativos, así como la digitalización de los datos personales de la sociedad, las políticas cero papel en los servicios públicos, la ficha electrónica judicial y el expediente electrónico en el sistema de justicia, el teletrabajo, la telemedicina, la teleducación, la polución de algoritmos, *smart city, smart contracts,* biotecnología, *blockchain*, transferencia de datos, *smart government*, ciberjusticia, *legaltech*, *e-commerce*, ODR, propiedad intelectual, ciberactivos, protección de datos y privacidad, la gobernanza de internet y la inteligencia artificial como tecnologías emergentes y disruptivas en la cotidianeidad de los servicios privados y públicos. ¿Qué derechos humanos se vulneran o limitan con la inminente «implementación de las sociedades tecnológicas»? Para ello, profundicemos un poco más en la IAG.

Algo que supera la imaginación es cuando a la IA le puedes pedir cree o dibuje un gato sino también te puede producir el sonido referencial correcto de un

gato con una red neuronal de IA. Se habla de «redes creativas» los *Deep fakes* de Tom Cruise. A verbigracia; la generación con IA de texto a audio (*text to audio*) o la clonación de la voz (*voice cloning*) permite recrear muestras de audios y voz de manera cíclica y constante siendo a veces imperceptible encontrar una diferencia con la voz originaria, por ejemplo, Leonardo Di Caprio hablando en las Naciones Unidas con diversidad de inflexiones de voz.

De similar manera, ChatGPT crea un texto realista logrando superar pruebas y logra antropobotizar[1] algorítmicamente para predecir la siguiente palabra con su lenguaje integrado con base en la pregunta que se realiza. Tal es así que la respuesta resulta ser única, incluso cuando dos personas realizan la misma pregunta, las respuestas serán diferentes.

Entonces, los *bots* aprenden de los seres humanos porque incrementan la información y la automaticidad de respuesta a medida de realizar diversas prácticas, es así que el uso de la tecnología y la IA impactaría en:

- El trabajo: la productividad humana creció como concepto desde la revolución industrial, con la determinación de horarios y periodos, para reiniciar el ciclo con IA las máquinas pueden tomar parte de nuestra productividad, significa suplir y desahogar tareas programáticas o que no se gusta hacer. Pero sí va a existir un reemplazo de personas en algunos espacios laborales impactando directa e indirectamente con el derecho al trabajo, acceso al trabajo y sindicalización.

  En el ámbito laboral el uso de la IA supera algunas tendencias así como el acercamiento con los robots. Por su parte, Oliver Bendel, profesor de Ética de la Tecnología y la Información en la Facultad de Economía FHNW (Suiza), mantiene una relación directa con los robots, pero sabe aún que no existe una dependencia a utilizarlos y sabe que en cualquier momento los podría desconectar. El XXI Congreso Internacional de Copardom sobre prevención de riesgos laborales (2023) tuvo como guía temática los retos digitales y sociales de la seguridad y la salud en el trabajo, donde se abordaron incertidumbres y algunas propuestas. La IA es un sistema innovador muy avanzado que posibilita la implementación de métodos destinados a la prevención de riesgos; pero es innegable que plantea también desafíos de cara a la vida laboral y mucho más allá.
- La educación: el uso de la IA es significativo, sin embargo, la preocupación del futuro será qué profesión podríamos recomendar a menores de edad, sobre todo pensar en áreas que no sean fácilmente reemplazadas por la IA, es decir, «profesiones que nos permitan crear condiciones para los seres humanos en el futuro 2050». Por ello, las ciencias de hoy no serán precisamente las profesiones del mañana con la inminente evolución de la IA. En efecto, la IA es un buen asistente en educación, la interacción entre el estudiante y el chat, logrando tener un tutor personalizado de forma permanente, tiene un alcance mayor, no veinte o treinta estudiantes, sino entre trescientos y quinientos estudiantes de forma virtual, como los programas de capacitación

1 Antropobotizar es una conjugación entre *antropo* (hombre) y *bot* (robot) que significa a través del pensamiento humano-robot.

MOOC. Es entonces posible reemplazar a un docente con un *teachbot*. Al parecer, el oficio de asistente es aceptable, pero reemplazar al docente quizá resulta ser más complejo porque es necesario algo más como el «cultivo del valor académico» a fin de evitar crear sociedades falsas, carentes de pensamiento crítico, conciencia, valor y moral.

- Identidad: el impacto de la IA en la identidad personal y los riesgos jurídicos que implican. Por ejemplo, *deep fake audio analysis*, que es la estructuración de personas sintéticas, seres creados con IAG adaptados con imagen y voz semejantes para interactuar con cualquier persona, como los proyectos de réplicas *metahuman post mortem*.

## Los derechos humanos y el uso de la IA

La proliferación de la IA plantea preocupaciones significativas en relación con los derechos humanos. Es por ello que los sistemas de IA pueden aprender prejuicios de los datos con los que se entrenan, afectando la equidad y justicia por un desequilibrio que rebasa la aplicación de una norma o la interpretación normativa sino que está afectada por la programación algorítmica.

Algunos DD. HH. implicados con la IA:

- Derecho a la dignidad: la IA y el poder público digital deberían seguir evolucionando sobre la base de que «todos los seres humanos nacen libres e iguales en dignidad y derechos, dotados de razonamiento y conciencia» para el ejercicio justo y equitativo como titular de sus derechos y libertades humanas.
- Derecho a la privacidad: la recopilación masiva de datos por parte de sistemas de IA puede comprometer la privacidad de las personas. La vigilancia masiva y la recopilación de datos personales sin consentimiento adecuado pueden violar el derecho a la privacidad.
- Derecho a la libertad de expresión: la IA también se utiliza para la moderación de contenido en plataformas en línea, lo que a veces puede resultar en la censura injusta o la limitación de la libertad de expresión de las personas.
- Derechos de autor y creación: la IA ha superado en gran medida lo imposible cuando se pretende explicar este punto; porque existe un sinfín de derechos que se debería garantizar desde los comprendidos en el Protocolo DESC; así como, garantizar los derechos del siglo XXI. Por ejemplo, la última canción con IA de 2023, de The Beatles, *Now and Then*.

A su vez, en el presente trabajo se busca determinar *prima facie* el impacto de la IA en los derechos humanos en Perú:

- Derecho a la dignidad y a la no discriminación, explicado letras antes.
- Privacidad y protección de datos: la recopilación y el procesamiento de datos personales por parte de sistemas de IA pueden plantear desafíos en cuanto a la privacidad de los ciudadanos peruanos. La Ley de Protección de Datos Personales y su reglamento, que se encuentra en plena implementación, es relevante en este contexto y busca proteger los derechos de privacidad de las personas.

- Derecho del Interés Superior del Niño, Niña y Adolescente: Organización Internacional del Trabajo (OIT), CADH, La Convención de los Derechos del Niño y en el ordenamiento interno la Ley 30.466, ley que establece parámetros y garantías procesales para la consideración primordial del interés superior del niño y su reglamento.

En resumen, la IA tiene un impacto significativo en los derechos humanos en Perú, tanto en términos de oportunidades como de desafíos. La regulación efectiva, la ética en la implementación de la IA y la sensibilización sobre estos temas son fundamentales para garantizar que la IA se utilice de manera justa y en beneficio de la sociedad peruana en su conjunto; para ello, es necesario asumir responsabilidad específicas y multipartitas de la mano con los especialistas en la materia a fin de garantizar los derechos humanos.

El vertiginoso cambio de las nuevas tecnologías por tecnologías emergentes y disruptivas está abriendo cambios transeccionales en distintas disciplinas, y el derecho no es ajeno a ello. Para Stéphane Pinon,

> de la materialidad de los derechos o del Estado constitucional estamos pasando al *constitucionalismo digital*. De igual forma, del constitucionalismo y la democracia de la *protección*, propia de la segunda mitad del siglo XX, la primera propia de Hans Kelsen, ya pasamos a la democracia constitucional de la participación. (Salcedo, 2023).

En este sentido, el constitucionalismo digital permitirá reconocer principios, derechos y valores constitucionales en entornos digitales. Es decir, encontrar nuevos paradigmas de control, representación y fiscalización social que corresponda a la «condición digital» actual de la humanidad. De similar forma, es necesario promover la investigación ética en relación a la IA a fin de desarrollar algoritmos y sistemas que sean «conscientes» de los sesgos y estén diseñados para minimizar la discriminación; sin importar que ahora los algoritmos sean programados por blancos y en el mañana lo realicen los negros o los de otro color, se considera también que estas opiniones conforman y fortalecen las diferencias raciales cuando ello ha quedado superado por el conocimiento y el desarrollo de los derechos humanos. A nivel de la Unión Europea, el Reglamento General de Protección de Datos busca abordar cuestiones relacionadas con la privacidad y la protección de datos en el contexto de la IA. El Reglamento ha influido en cómo las empresas e instituciones en Europa gestionan los datos personales y respetan los derechos de privacidad.

Finalmente, Declaración de Toronto busca aplicar las normas internacionales de los derechos humanos subsistentes con la IA o de aprendizaje automático, considerado como un referente; por lo que es indispensable promover un compromiso de los gobiernos y de las empresas para garantizar que los algoritmos se apliquen de forma equitativa y quienes se encuentren afectados tengan una vía legítima, legal y pertinente para su reparación.

## Conclusiones

La IA es una potente tecnología y de alcance global que evoluciona en niveles de mayor capacidad, incluso mayor que la propia capacidad del ser humano, y aprende en el menor tiempo posible.

Los seres humanos no debemos competir con las máquinas, pero sí debemos optimizar nuestras habilidades, fortalecer nuestro conocimiento y potenciar nuestra evolución utilizando a las tecnologías y a la IA como herramientas útiles para nuestra proyección de vida.

Los organismos internacionales están trabajando para garantizar los derechos humanos, las empresas tienen que asumir compromisos de responsabilidad solidaria, los gobiernos implementar políticas y normativas garantes, la ciudadanía formar una cultura digital proteccionista y antropocentrista.

Evitar que el avance de la IA no se conviertan en amenazas para sus destinatarios o en intrumentos de ataque de forma insdicriminada e irreparable.

La educación y la concienciación pública son decisivos para empoderar a las personas en el uso de la IA y así garantizar la protección de sus derechos humanos.

La responsabilidad civil y penal recae en los gobiernos, las organizaciones y la sociedad en su conjunto para garantizar que la IA se utilice de manera ética y en beneficio de todos los habitantes en Perú y en otros países.

Sugiero aplicar la teoría de la «triple hélice» para resolver inicialmente todos los problemas que surjan de la IA; sin embargo, después de superar este nivel de resolución de conflictos, se propone trabajar en la «quíntuple hélice» de forma colaborativa con la academia, las empresas, los gobiernos y las ONG; así como en el Impacto al Medio Ambiente.

## Referencias bibliográficas

Canales, K. (2023). Foro de comercio e innovación, Corea-LAC-2. *BID*. https://www.youtube.com/watch?v=RiU_CThK69M

Gil Domínguez, A. (11 de junio, 2023). Adelanto de «Constitucionalismo digital», el nuevo libro de Andrés Gil Domínguez. *Infobae*. https://www.infobae.com/judiciales/2023/06/11/adelanto-de-constitucionalismo-digital-el-nuevo-libro-de-andres-gil-dominguez/

Grigore, A. E. (2022). Derechos humanos e inteligencia artificial. *Ius Et Scientia*, *8*(1), 2022, 164-175. https://doi.org/10.12795/IETSCIENTIA.2022.i01.10

High, R. (2023). *La Era de los Sistemas Cognitivos: Una mirada al interior de IBM Watson y ¿Cómo funciona?* Redbooks. https://www.redbooks.ibm.com/redpapers/pdfs/redp4955_es.pdf

Nikken, P. (1994). *El Concepto de Derechos Humanos. Estudios Básicos de Derechos Humanos*. Instituto Interamericano de Derechos Humanos. https://perio.unlp.edu.ar/catedras/iddi/wp-content/uploads/sites/152/2020/08/1-Nikken-El-Concepto-de-Derechos-Humanos.pdf

Núñez, J. (2021). Innovación digital en el Poder Judicial en el Perú: Aplicación de las nuevas tecnologías transformadoras y disruptivas. *Revista Iberiamericana de Informática y Derecho, 2*(11). https://revistas.fcu.edu.uy/index.php/informaticayderecho/article/view/3045/2610

Ortega García, R. (2013). La constitucionalización del derecho en México. *Boletín de Mexicano de Derecho Comparado*, *43*.

Rudas Murga, C. (2017). Siglo XXI: la «googlización» de los Wikileaks en el mundo. *Revista perspectiva*, *17*(3), https://revistas.upagu.edu.pe/index.php/PE/article/view/435

Salcedo Camacho, C. (2023). Retos éticos, derechos humanos y democracia en el constitucionalismo digital. *Acento SAS*. https://acento.com.do/opinion/retos-eticos-derechos-humanos-y-democracia-en-el-constitucionalismo-digital-9255771.html

Zhang, T. (18 de mayo, 2022). GDPR Versus PIPL. Key Differences and Implications for Compliance in China. *China Briefing from Dezan Shira and Associates*. https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 137-154

# *BLOCKCHAIN* Y LA SEGURIDAD DE LA INFORMACIÓN EN AMÉRICA Y EUROPA

*BLOCKCHAIN AND INFORMATION SECURITY IN AMERICA AND EUROPE*

**Alexis G. Antoniucci**
**Manfry R. Sierra Alemán**
**Jesús Báez**
**Michele Crisafulli**
Miembros de Primeros en FIADI

## Resumen

La tecnología *blockchain* puede cambiar las reglas del juego en los sectores relacionados con la seguridad y la gestión de la información, ya que es descentralizada, inmutable y segura. La *blockchain* parece ser una solución extremadamente potencial para alcanzar una mayor integridad y confidencialidad de los datos. Gobiernos de todo el mundo están trabajando en la implementación de la *blockchain* en sus respectivos sistemas. Colombia y República Dominicana son solo algunos de los que están explorando el potencial de la *blockchain* en relación con aspectos como los sistemas de votación, la adopción de criptomonedas o la gestión de la cadena de suministro, entre otros. La Unión Europea, por otro lado, está adoptando un enfoque complejo de la regulación de la *blockchain*, tratando de equilibrar la innovación con la protección de los datos personales. Italia ha aprobado legislación que menciona explícitamente la DLT, apreciando el potencial de la tecnología para mejorar la transparencia y la eficiencia en una serie de ámbitos. Aunque las posibilidades de que la *blockchain* ofrezca grandes oportunidades son considerables, existen retos evidentes en términos de interoperabilidad, escalabilidad y claridad jurídica. Esto exige flexibilidad en los marcos reguladores para detener estos retos y apoyar un desarrollo responsable. En general, la cadena de bloques tiene un enorme potencial disruptivo en el ámbito de la seguridad y la gobernanza, entre otras muchas industrias, pero requiere la colaboración de gobiernos, industrias y la comunidad jurídica para convertirse en un verdadero éxito.



## Palabras clave

*Blockchain*, tecnología disruptiva, seguridad, interoperabilidad, marco regulatorio.



## Abstract

Blockchain technology can be a game-changer for security and information for management-related industries because it is decentralised, immutable, and secure. Blockchain seems to be an extremely potential solution to improve data integrity and confidentiality. Governments worldwide are working on implementing blockchain in their respective systems. Colombia and the Dominican Republic are but an example of those exploring blockchain's potential in regard to voting systems, cryptocurrencies, and supply chain management, among others. The European Union, on the other hand, is taking a complex approach to the regulation of blockchain, seeking to balance innovation with protection of personal data. Italy has passed legislation explicitly mentioning DLT, appreciating the potential of the technology to improve transparency and efficiency in a number of areas. While there are considerable opportunities arising from blockchain, obvious challenges exist in terms of interoperability, scalability, and legal clarity. This calls for flexibility in regulatory frameworks in order to arrest these challenges and support responsible development. Overall, blockchain does have a huge potential for disruption in the security and governance area, among many other industries, but it calls for collaboration between governments, industries, and the legal community if it is to turn into a real success.



## Keywords

Blockchain, disruptive technology, security, interoperability, comparison, regulatory framework.

## Introducción

La seguridad de la información es un pilar fundamental en la era digital, donde la integridad, confidencialidad y disponibilidad de los datos se han convertido en aspectos cruciales para el funcionamiento de las sociedades modernas. En este contexto, la tecnología *blockchain* emerge como una solución prometedora debido a su capacidad para ofrecer una estructura de datos inmutable y descentralizada, lo que potencialmente puede transformar la manera en que se maneja la seguridad de la información tanto en América como en Europa.

La adopción de *blockchain* en diversas industrias ha demostrado su versatilidad, y su aplicación en la seguridad de la información no es una excepción. Esta tecnología, originalmente concebida para sustentar la criptomoneda Bitcoin, ha evolucionado para abarcar una amplia gama de aplicaciones que van más allá de las finanzas, incluyendo la gestión de identidades, la logística y la protección de propiedad intelectual, entre otros.

Sin embargo, la implementación de *blockchain* en sistemas de seguridad de la información no está exenta de desafíos. La regulación, por ejemplo, juega un papel determinante en la forma en que se utiliza y se le da alcance a esta tecnología. Las diferencias regulatorias entre América y Europa pueden influir significativamente en la adopción y adaptación de *blockchain*, así como en las prácticas de seguridad de la información en general.

En América, con un enfoque más orientado hacia la innovación y la flexibilidad regulatoria, vemos un rápido avance en la implementación de *blockchain*, lo que permite a las empresas y organizaciones explorar nuevas formas de proteger sus datos. Por otro lado, Europa, con su riguroso marco de protección de datos personales establecido por el Reglamento General de Protección de Datos (GDPR), presenta un escenario más cauteloso, donde la seguridad de la información y la privacidad son prioridades absolutas.

El análisis de cómo se entiende y se trata la tecnología *blockchain* en el contexto de la seguridad de la información es, por tanto, indispensable. No solo es necesario comprender su funcionamiento técnico, sino también el impacto que tiene en las políticas de seguridad, las estrategias de mitigación de riesgos y la cultura de seguridad en las organizaciones.

La regulación adecuada de *blockchain* podría armonizar los beneficios de esta tecnología con las necesidades de seguridad de la información, creando un equilibrio entre la innovación y la protección de datos. Esto es especialmente relevante en un mundo cada vez más interconectado, donde las brechas de seguridad no conocen fronteras y sus consecuencias pueden ser globales.

Por lo tanto, es fundamental que los responsables de la formulación de políticas, los profesionales de la seguridad de la información y los desarrolladores de *blockchain* trabajen conjuntamente para establecer estándares y prácticas que maximicen las ventajas de la tecnología *blockchain*, al tiempo que se minimizan sus riesgos. Solo así podremos asegurar que la seguridad de la información en América y Europa esté a la altura de los desafíos que presenta el siglo XXI.

## El caso de Colombia

La trascendencia radica en que esta tecnología está teniendo una gran acogida y aplicabilidad por distintos actores que han entendido el potencial de esta (proyectos piloto, índices globales, etc.). En ese sentido, el estado colombiano ha venido tomando cartas, ya que se ha entendido que en esta denominada 4º Revolución Industrial las tecnologías juegan un factor clave y trascendental para generar valor agregado hacia la sociedad. Hablando de esa transformación, entendida como transformación digital (de la sociedad) se encuentran:

- La Ley 1955/19 (PND 18-22) en su artículo 147, numerales 6 (priorización de tecnologías emergentes de la Cuarta Revolución) y 11 (inclusión y actualización permanente de políticas de seguridad y confianza digital).
- La Guía de Referencia para la adopción e implementación de proyectos con tecnología *blockchain* para el Estado colombiano (Versión del 2 de mayo de 2022), que corresponde a un instrumento de derecho blanco en el marco del Decreto 767 de 2022.
- La Ley 2294/23: financiamiento para la acción climática, se crearán los incentivos y mecanismos donde se implementen líneas de crédito más amplias y con tasas compensadas, con fondos de financiamiento combinado, para proyectos climáticos de gran impacto con uso de tecnología *blockchain*.

## 1. Blockchains abiertas (públicas)

Cualquiera puede leer un *blockchain* público, enviar transacciones o participar en el proceso de consenso. Se los considera «sin permiso». Todas las transacciones son públicas y los usuarios pueden mantenerse anónimos en algunas aplicaciones.

Ventajas:

- Todo aquel que quiere puede obtener copias de las transacciones, ya que están distribuidas entre todos los participantes.
- Todo aquel que así lo desee puede unirse a la red.
- Al ser redes públicas, todos los participantes tienen los mismos derechos y nadie está a cargo o tiene alguna propiedad especial.
- Nadie puede cambiar o manipular los datos una vez han sido registrados.

Desventajas:

- Alto consumo energético.
- Todas las transacciones pueden ser rastreadas hasta una misma billetera, aunque en la mayoría de los casos no supone un problema dado que las cuentas suelen ser anónimas.
- Se debe pagar comisión a los mineros para realizar transacciones.

## 2. Blockchains cerradas

Son controlados por una única organización o consorcio que determina quién puede leerlos, presentar transacciones en este y participar en el proceso de consenso.

Ventajas:

- Poseen mayor rendimiento, lo que se traduce en velocidad, porque la cantidad de actores en la red es menor.
- Dado que son redes privadas, el anonimato no existe y presenta un mayor nivel de confiabilidad.
- Los usuarios no deben pagar comisión por el uso de la red.

Desventajas:

- Los registros se encuentran centralizados totalmente y son de acceso cerrado, por lo que pertenecen a una única entidad u organización.

## 3. Usos de la tecnología *blockchain* en Colombia

### *3.1. Democracia (sistemas de votación electoral)*

Un ejemplo práctico realizado en Bogotá en 2018, apoyado y galardonado por parte del MinTIC, se realizó con la elección de personeros en dos instituciones educativas, en el que se desarrolló el proceso electoral existente bajo la tecnología *blockchain*. La Alta Consejería Distrital de TIC y la Secretaría Distrital de Educación, a través de ViveLab Bogotá, desarrollaron un proceso experimental para el desarrollo de elecciones digitales de representante estudiantil, haciendo uso de *blockchain*.

### *3.2. Contratación (transparencia)*

La Procuraduría General de la Nación junto con el Banco Interamericano de Desarrollo y el Foro Económico Mundial lideraron un equipo multidisciplinario que desarrolló el «Proyecto de la Transparencia» (*Transparency Project*) en el que conjuntamente diseñaron un *software* piloto (*proof-of-concept* o POC) basado en la tecnología *blockchain* que pretende ser implementado en los procesos de selección que se lleven a cabo mediante el Sistema de Compras Públicas colombiano, con el fin de aumentar la transparencia y reducir el riesgo de corrupción. El enfoque del proyecto tiene tres componentes fundamentales: *software* de POC basado en tecnología *blockchain* para licitaciones públicas; recomendaciones de índole legal, de políticas y gobernanza y apropiación de la sociedad civil y participación estratégica.

### *3.3. Educación*

A través de la Red *UxTIC.co*, las universidades se han unido para formar un grupo de trabajo *blockchain*, con el propósito de incrementar los niveles de adopción y transferencia de conocimientos desde la academia. Dentro de las

actividades desarrolladas por este grupo está la realización de un *tour* universitario, en el que participaron doce universidades, para hacer el levantamiento de los proyectos en la academia o en colaboración con el sector privado o público; dentro de los resultados se encontraron más de veinte proyectos realizados por investigadores y alumnos, varios de ellos en alianza con otras universidades o empresas en Colombia o el exterior.

En agosto del 2022, se llevó a cabo la prueba piloto de emisión de bonos usando tecnología *blockchain*. El objetivo de esta prueba, que se constituye en la primera de este tipo en la región, fue observar el impacto de la Tecnología de Registro Distribuido (DLT) utilizando contratos inteligentes, un *token* no fungible y algoritmos de cifrado a lo largo de todo el ciclo de vida de un bono en el segundo mercado, en términos de costos operacionales, tiempos, trazabilidad, documentación y asimetrías de información hacia los participantes, entre otros. La Super Intendencia Financiera de Colombia, catalogó el piloto como exitoso, teniendo en cuenta que la autorización, inscripción inicial y posterior cancelación en el Registro Nacional de Valores y Emisores (RNVE), así como la emisión, negociación, registro de pagos y cumplimiento, se realizaron en su totalidad con tecnología *blockchain* de manera ágil y segura.

### 4. Caso de estudio de uso de la tecnología blockchain

La Ley 2294 del 2023, Plan Nacional de Desarrollo (PND), que es el documento que constituye la base y provee lineamientos estratégicos para la formulación de políticas públicas por el gobierno nacional, es el instrumento formal y legal por medio del cual se trazan los objetivos del gobierno. En el programa de gobierno se apuntó a la implementación de tecnologías como *blockchain*, entre otras, para el financiamiento climático neto, como motor para el desarrollo sostenible, donde se espera asignación de recursos energéticos renovables.

Esto, conforme al plan de inversiones bajo el programa de integración de energías renovables para Colombia, con ello, se espera el escenario más ambicioso bajo el Plan Energético Nacional 2020-2050 de Colombia, adoptado por el PIGCCME, busca reducir las emisiones en 31,6 MTCO2E para 2050. Las líneas de actuación incluyen la implementación de tecnologías disruptivas, donde la adopción de transacciones tipo *blockchain* y la implementación de centros de control autónomos

## El caso de República Dominicana

### 1. Definición de blockchain en la República Dominicana

En la República Dominicana, *blockchain* se define como una tecnología de registro distribuido que permite la creación de un libro de transacciones inmutable y seguro sin la necesidad de una autoridad central. Esta definición destaca las características fundamentales de *blockchain*: la descentralización, la inmutabilidad y la seguridad de los datos registrados.

## 2. Funcionamiento y trascendencia

*Blockchain* funciona mediante una red de nodos que validan y registran transacciones en bloques, los cuales están enlazados de manera secuencial y segura a través de criptografía. Este proceso garantiza que una vez que la información se ha registrado en la cadena, no puede ser alterada sin el consenso de la mayoría de los nodos, lo que refuerza su seguridad y fiabilidad.

## 3. Blockchains abiertas

Las *blockchain*s abiertas son redes públicas donde cualquier persona puede participar en el proceso de verificación de transacciones. Estas redes son completamente descentralizadas y permiten la participación abierta, lo que las hace transparentes, pero también vulnerables a ciertos tipos de ataques si no se aplican medidas de seguridad adecuadas.

## 4. Blockchains cerradas

Las *blockchain*s cerradas, por otro lado, son redes privadas o permisionadas donde el acceso está restringido a entidades autorizadas. Este modelo ofrece mayor control y seguridad, siendo ideal para aplicaciones donde la privacidad y la gestión de acceso son críticas.

En la República Dominicana, la trascendencia de *blockchain* ha sido cautelosa, con un enfoque regulatorio aún en desarrollo. Sin embargo, ha habido un notable incremento en el interés y la adopción de criptomonedas y tecnología *blockchain*, reflejando una tendencia global hacia la digitalización de la economía.

## 5. Usos de la tecnología blockchain en la República Dominicana

### *5.1. Sistemas de votación electoral*

Aunque no existe evidencia de la implementación actual de *blockchain* en sistemas de votación electoral en la República Dominicana, esta tecnología tiene el potencial de ofrecer transparencia y seguridad en los procesos electorales, asegurando que cada voto sea registrado y contabilizado de manera inmutable.

### *5.2. Criptomonedas*

El uso de criptomonedas ha visto un incremento en el país, a pesar de las advertencias del Banco Central de que estas no cuentan con respaldo oficial. Esta creciente adopción refleja la popularidad y la confianza en las criptomonedas como una forma alternativa de inversión y ahorro.

### *5.3. Activos virtuales y finanzas descentralizadas*

La presencia de activos virtuales y finanzas descentralizadas (*DeFi*) en la República Dominicana enfrenta desafíos regulatorios y de adopción. Aun así,

estos sistemas representan una oportunidad para democratizar el acceso a servicios financieros y mejorar la inclusión financiera.

### *5.4. Oportunidades para la transparencia*

La tecnología *blockchain* puede ofrecer significativas oportunidades para la transparencia y eficiencia en la administración pública y el comercio exterior. Al proporcionar un registro inmutable y transparente de las transacciones y documentos, *blockchain* puede ayudar a combatir la corrupción y mejorar la confianza en las instituciones públicas.

## 6. Caso de estudio: adopción de criptomonedas en la República Dominicana

Un informe reciente resalta un aumento del 52% en la adopción de criptomonedas en 2022 en la República Dominicana. A pesar de la falta de regulación específica, hay un interés creciente en la educación sobre criptomonedas y *blockchain*. Los ingresos generados a través de criptomonedas en 2022 alcanzaron los 10,36 millones de dólares, con un 2,08% de la población poseyendo criptomonedas.

### *6.1. Regulación*

El Banco Central de la República Dominicana ha advertido que ninguna criptomoneda cuenta con el respaldo oficial de la Junta Monetaria, lo que significa que no tienen curso legal ni fuerza liberatoria de obligaciones en el país. Esta postura refleja una cautela hacia la adopción masiva sin un marco regulatorio sólido.

### *6.2. Ventajas*

Entre las ventajas de la tecnología *Blockchain* se encuentran la transparencia, la inmutabilidad de los datos y la eliminación de intermediarios, lo que puede reducir costos y aumentar la eficiencia en diversas aplicaciones, desde transacciones financieras hasta la gestión de cadenas de suministro.

### *6.3. Desventajas*

Sin embargo, también existen desventajas, como la alta volatilidad de las criptomonedas, los riesgos de fraude y estafas, y la falta de una regulación clara que pueda proporcionar seguridad jurídica a los usuarios.

### *6.4. Blockchain y la seguridad de la información*

La tecnología *blockchain* representa un avance significativo para la seguridad de la información en diversos sectores, especialmente en el contexto de la digitalización. Su estructura descentralizada y la criptografía avanzada ofrecen una protección robusta contra la manipulación y el acceso no autorizado. En la República Dominicana, donde la digitalización está en curso, *blockchain* puede

ser una herramienta valiosa para asegurar datos sensibles en sectores como la salud, la banca y el gobierno.

### *6.5. Inclusión de la blockchain en la Administración Pública*

La inclusión de *blockchain* en la administración pública dominicana puede transformar la forma en que se manejan los datos y se realizan las transacciones. Con su capacidad para crear registros inmutables y transparentes, *blockchain* puede mejorar la eficiencia, reducir la burocracia y aumentar la confianza en las instituciones públicas. Aunque la adopción de esta tecnología en la administración pública aún está en sus etapas iniciales, existe un potencial considerable para su uso en la gestión de registros civiles, licitaciones públicas y otros procesos administrativos.

### *6.6. Blockchain y la transparencia administrativa*

La implementación de *blockchain* en la Administración Pública puede contribuir significativamente a la transparencia. Al automatizar y registrar cada transacción o acción administrativa en una cadena de bloques, se reduce la posibilidad de corrupción y se facilita la auditoría y el seguimiento de los procesos. Esto es particularmente relevante en la República Dominicana, donde la transparencia y la lucha contra la corrupción son prioridades clave para el desarrollo sostenible.

### *6.7. Educación y regulación*

Para que la tecnología *blockchain* alcance su máximo potencial en la República Dominicana, es crucial promover la educación y establecer un marco regulatorio claro. La educación permitirá a los ciudadanos y a los funcionarios comprender y adoptar esta tecnología de manera efectiva, mientras que una regulación adecuada proporcionará seguridad jurídica y fomentará la innovación responsable.

## 7. Conclusiones

*Blockchain* tiene el potencial de fortalecer la seguridad de la información y revolucionar la Administración Pública en la República Dominicana. Sin embargo, para lograr estos beneficios, es esencial una estrategia integral que incluya educación, regulación y colaboración entre diferentes sectores. La promoción de la educación financiera y tecnológica es esencial para una regulación efectiva. La comprensión de las criptomonedas y de la tecnología *blockchain* entre la población dominicana permitirá tomar decisiones informadas y responsables. La colaboración entre el gobierno, entidades financieras y la comunidad cripto será clave para construir un entorno regulatorio que fomente la confianza y el progreso, beneficiando la economía dominicana y a sus ciudadanos.

## El caso de Italia

### 1. Ventajas y características de la cadena de bloques

La tecnología de cadena de bloques revoluciona la tesis clásica según la cual la certidumbre de una relación jurídica entre particulares sólo puede garantizarse mediante la intervención de un tercer organismo que sea *super partes*.

Dentro del libro mayor distribuido creado por la cadena de bloques, cada transacción es validada por el consenso generalizado de los demás participantes en la red, conocidos como «nodos». Solo cuando la transacción es aprobada por la totalidad o mayoría de los nodos, constituirá un nuevo «bloque», actualizando así la cadena.

Normalmente la identidad de los usuarios que aprueban o realizan la transacción está protegida mediante un proceso de seudonimización, que permite rastrear únicamente a la clave alfanumérica pública que los identifica, pero no a sus datos personales.

Otra ventaja de la cadena de bloques es que el registro distribuido no se almacena a través de una estructura jerárquica *server-client*, en la que el único propietario de la *blockchain* es el organismo centralizado, sino que sigue un esquema *peer-to-peer*, en el que el registro es compartido y accesible entre todos los nodos y modificable sólo a través del proceso de aprobación mediante el consenso generalizado que se acaba de explicitar. Por último, una vez que se ha producido una nueva transacción dentro del registro distribuido, esta adquiere el carácter de inmutabilidad, ya que cada nuevo bloque incluye las cadenas de todos los bloques anteriores, hasta el primer bloque. De este vínculo inseparable entre bloques pasados y bloques futuros se deriva la inmutabilidad de la cadena.

De estos elementos se deducen las características revolucionarias en las que se basa la tecnología *blockchain*: descentralización, transparencia, seguridad, inmutabilidad, consenso generalizado y ausencia de cualquier autoridad central encargada de gestionar y controlar el registro distribuido.

### 2. La cadena de bloques en la legislación europea

La Unión Europea ha declarado su intención en convertirse en líder en la tecnología *blockchain* y, por eso, ha adoptado un enfoque polifacético para regular esta tecnología a través de la combinación de iniciativas legislativas y medidas de promoción y apoyo.

Desde la perspectiva jurídica, las dos intervenciones más significativas son el Reglamento UE 2022/858 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y el Reglamento UE 2023/1114 relativo a los mercados de criptoactivos (*MiCA*). Aunque se encargan de reglamentar la cadena de bloques en sectores específicos y no constituyen una ley general sobre el tema, es importante analizar, en manera sintética, las normas más significativas.

El Reglamento del 2022 tiene por objeto eliminar los obstáculos a la emisión y negociación de instrumentos financieros en forma de cripto activos y

garantizar que las autoridades de la UE adquieran experiencia en el uso de los TRD en los sistemas multilaterales de negociación y liquidación. El modelo de infraestructuras de mercado configurado por la *MiFID II* y el *MiFIR* es de carácter centralizado e impide aplicar esta normativa a la transmisión en centros de negociación de instrumentos financieros representados por criptoactivos. El Reglamento pretende solucionar esta cuestión al establecer un régimen piloto que permita la creación de infraestructuras de mercado basadas en la TRD. Se trata de la primera en aplicarse entre las tres iniciativas legislativas anunciadas por la Comisión Europea con el denominado Paquete de Finanzas Digitales adoptado el 24 de septiembre de 2020.

En el artículo 2 de este Reglamento se pueden encontrar algunas importantes definiciones:

> *Tecnología de registro descentralizado* o TRD: una tecnología que permite el funcionamiento y el uso de registros descentralizados.
>
> *Registro descentralizado*: un repositorio de información que lleva registros de operaciones y se comparte a través de un conjunto de nodos de red TRD y está sincronizado entre dichos nodos, utilizando un mecanismo de consenso.

Es crucial entender la diferencia entre TRD y *blockchain*. La *blockchain* es solo un tipo de tecnología de registro descentralizado. Una TRD no tiene que estar necesariamente formada por una secuencia de bloques, por lo que la *blockchain* es solo un subconjunto de ella. En general, la tecnología de registros distribuidos puede definirse utilizando el mismo concepto que la *blockchain*, pero mientras que todas las *blockchain*s son *distributed ledgers*, no todos los *distributed ledgers* son *blockchains*. Esta diferencia se subraya también en el documento de la Organización Internacional de Normalización ISO/23257:2022, donde se afirma que «una plataforma Blockchain es una plataforma DLT en la que la tecnología utilizada es la Blockchain». Así que el Reglamento tiene por objeto todas las tecnologías de registros descentralizados y, de consecuencia, la *blockchain*.

El Reglamento *MiCA* establece normas uniformes para los emisores de cripto activos y para los proveedores de servicios en relación con los cripto activos. Este Reglamento hace referencia expresa a la tecnología de cadena de bloques solo en el considerando 1, donde se afirma que:

> La Unión tiene un interés estratégico en desarrollar y promover la adopción de tecnologías transformadoras en el sector financiero, incluida la adopción de la tecnología de registro distribuido (TRD). Se espera que muchas aplicaciones de la tecnología de registro distribuido, incluida la tecnología de cadena de bloques, que aún no han sido estudiadas en su totalidad sigan creando nuevos tipos de actividad empresarial y modelos de negocio que, junto con el propio sector de los criptoactivos, generarán crecimiento económico y nuevas oportunidades de empleo para los ciudadanos de la Unión.

La primera observación es que, en el ámbito legislativo, la Unión Europea está interviniendo más eficazmente en todos los sectores en que la tecnología de cadena de bloques encuentra intereses económicos y financieros. No obstante, como se verá más adelante, hay muchas otras iniciativas y directrices no vinculantes para fomentar el uso de esta tecnología.

## 3. La cadena de bloques en la legislación Italiana

En Italia, algunas leyes hacen referencia expresa a la tecnología de registros distribuidos. En primer lugar, se debe mencionar el artículo 8 *ter* de la L. 12 del 11 Febrero 2019, que describe las TRD con la siguiente definición:

> Tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili[1].

La misma ley, solo a título informativo, define también al *smart contract* como «un programa informático que funciona con tecnologías basadas en registros distribuidos y cuya ejecución vincula automáticamente a dos o más partes, basándose en basándose en efectos predefinidos del mismo» (traducción propia). Esta definición jurídica, a diferencia de la de antes, es muy confundida y técnicamente incorrecta por varias razones. En primer lugar, porque se crea erróneamente un vínculo lógico inseparable entre contratos inteligentes y *blockchain*. De hecho, un *smart contract* puede existir de forma independiente respecto de la cadena de bloques. En segundo lugar, el legislador inserta una norma capaz de tener un fuerte impacto en el derecho contractual, sin haber aclarado previamente el alcance de la conexión que existe entre los contratos inteligentes y el derecho contractual tradicional.

Otra mención más reciente a la cadena de bloques se hace en la Ley 206/2023, donde se dice que el Ministerio del *Made en Italy* apoya el desarrollo y el uso de tecnologías basadas en registros distribuidos. Esta norma identifica en esta tecnología una herramienta útil para garantizar la trazabilidad y la valorización de la cadena de suministro del *Made in Italy* con el fin de mejorar la exhaustividad y fiabilidad de la información a disposición de los consumidores. Con esta finalidad se constituye un catálogo nacional para monitorizar todas las iniciativas tecnológicas. El objetivo es fomentar la interoperabilidad con todas las otras soluciones desarrolladas en el ámbito de la Unión europea.

## 4. Otras iniciativas y aplicaciones de la blockchain en la Unión Europea

Aparte de los reglamentos en el sector financiero, la Unión Europea avanza con otras iniciativas para garantizar el correcto empleo y la interoperabilidad de las tecnologías basadas en la cadena de bloques en todo su territorio. Cabe mencionar, sobre todo, dos iniciativas principales: la Infraestructura Europea de Servicios Blockchain (EBSI) y el Sandbox Regulador Europeo para Blockchain.

1 «Tecnologías y protocolos informáticos que utilizan un registro compartido, distribuido, replicable, accesible simultáneamente, estructuralmente descentralizado sobre una base criptográfica, de forma que los datos puedan registrarse, validarse, actualizarse y almacenarse tanto de forma abierta, como protegida por un cifrado verificable por cada participante, de manera que no puedan alterarse ni modificarse». Traducción de los autores.

El primer proyecto tiene como objetivo crear un sistema paneuropeo de servicios públicos basados en tecnología *blockchain.* Este proyecto nació después de la creación de la Asociación Europea de Blockchain (EBP). La red *blockchain* EBSI es específica de varias maneras clave: a) está autorizada, lo que significa que no cualquiera puede operar un nodo EBSI, y nadie puede escribir información sobre él, esto evita que EBSI se utilice con fines ilegales; b) es soberano y tiene su sede en la UE, lo que significa que todos los nodos EBSI tienen su sede en Europa y EBSI cumple con los valores y regulaciones europeos, como GDPR; c) debido a que hay menos actores autorizados involucrados, EBSI es energéticamente eficiente. Utiliza un método de consenso basado en la prueba de autoridad, que casi no requiere potencia de cálculo y que, a diferencia de la minería pública ilimitada en todo el mundo, consume poca energía. Los actuales casos de uso de esta infraestructura europea se refieren a estos sectores:

a) notarización: crear pistas de auditoría digitales confiables, automatizar las verificaciones de cumplimiento en procesos críticos y garantizar la integridad de los datos;

b) diplomas: apoyar el ciudadano en la gestión de sus credenciales educativas, reduciendo los costes de verificación y mejorando el nivel de confianza en la autenticidad;

c) identidad digital europea: permitir a los usuarios crear y controlar su propria identidad digital a través de las fronteras y sin depender de autoridades centralizadas;

d) intercambio de datos de confianza: compartir los datos de forma segura entre las autoridades de la Unión.

Por último, la Unión Europea está desarrollando el Sandbox Regulador Europeo para Blockchain. Con el término *sandbox* se define un entorno controlado donde las empresas pueden probar productos y servicios mientras se relacionan con los reguladores. El objetivo es facilitar a los reguladores y supervisores la ampliación de su comprensión sobre las tecnologías de *blockchain* más avanzadas y fomentar el intercambio de las mejores prácticas mediante un diálogo continuo, antes de la implementación a gran escala.

## Conclusiones

La tecnología *Blockchain* representa una gran oportunidad para las empresas y para todas las autoridades del sector público. Los desafíos técnicos principales se conectan con la necesidad de garantizar la interoperabilidad entre las diferentes redes y protocolos y la escalabilidad, o sea la posibilidad de gestionar un número mayor posible de transacciones sin comprometer la seguridad de la red.

Por otro lado, el derecho tiene que idear soluciones adecuadas a las nuevas situaciones jurídicas que se van configurando para poder hacer frente a los retos que plantean estas tecnologías. Las principales cuestiones están conectadas con la necesidad de crear un paradigma legal que sea sencillo y claro en las definiciones y en la creación de los conceptos jurídicos. La falta de claridad en

la formulación de las normas puede alejar las empresas que operan en este sector. La ley debe también garantizar que se puedan implementar exclusivamente soluciones que garanticen altos estándares de seguridad en la protección de la privacidad de los usuarios.

Cabe por último subrayar que la estrategia futura de la Comisión Europea quiere apoyar un «estándar de oro» para la tecnología *blockchain* en Europa que abarque los valores e ideales europeos en su marco legal y regulatorio. El respeto de este estándar, de acuerdo con lo que se ya se ha dicho, incluye la sostenibilidad medioambiental, la ciberseguridad, la mejora de la identidad digital en Europa, la eficaz protección de los datos y la interoperabilidad de los sistemas entre Estados.

## Referencias bibliográficas


Alcaldía de Bogotá. (2023). *Implementación del prototipo Blockchain para procesos electorales en colegios públicos*. (2.ª ed.). https://tic.bogota.gov.co/sites/default/files/2023-11/*blockchain*para_elecciones.pdf

Banco Central de la República Dominicana. (30 de septiembre, 2021). *Comunicado sobre criptomonedas y monedas y activos virtuales*. https://bancentral.gov.do/a/d/5196-comunicado-sobre-criptomonedas-y-monedas-y-activos-virtuales

Banco de la República. (22 de agosto, 2022). *El Banco de la República participó en la emisión del primer bono en blockchain de Colombi*a. https://www.banrep.gov.co/es/noticias/banco-republica-participo-emision-primer-bono-blockchain-colombia

Bancos, Finanzas y Valores. (18 de septiembre, 2023). Informe señala aumenta en Dominicana el interés por las criptomonedas y blockchain. *Bancos Finanzas y Valores*. https://bancosfinanzasvalores.com/2023/09/18/republica-dominicana-aumenta-el-interes-por-las-criptomonedas-y-blockchain-segun-nuevo-informe/

Campo, H. (2021). Blockchain: Brindando confianza y transparencia. *PwC*. https://www.pwc.com/ia/es/publicaciones/perspectivas-pwc/Blockchain-brindando-confianza-y-transparencia.html

Canducci, M., Isaja, M., Carotenuto, A., Idone, G., Abbiati, E., Tarantino, U., Croce, V., Russo, M. (s. f.). *Unchaining business through the Blockchain*. Engineering. https://www.eng.it/resources/whitepaper/doc/blockchain/Blockchain_whitepaper_it.pdf

Cappiello Benedetta, A. R. (2020). Dallo "Smart Contract" computer code allo smart (legal contract). I nuovi strumenti (para) giuridici alla luce della normativa nazionale e del diritto internazionale privato europeo: prospettive de jure condendo *Diritto del commercio Internazionale*, 2/2020, p. 477 y ss.

Chomczyk, A. (2020). *Regulación de blockchain e identidad digital en América Latina: El futuro de la identidad digital*. Banco Interamericano de Desarrollo. https://publications.iadb.org/es/publications/spanish/viewer/

Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf

Colombia. Ministerio de Tecnologías de la Información y Comunicaciones. (2022). *Guía de Referencia para la adopción e implementación de proyectos con tecnología Blockchain para el Estado colombiano*. https://gobiernodigital.mintic.gov.co/692/articles-272783_recurso_1.pdf

De Leo, M., Biscaretti Di Ruffia, B. (13 de julio, 2022). Il regime pilota per le infrastrutture di mercato basate su blockchain e altre DLT: un segnale per il settore finanziario europeo. *NT Diritto*. https://ntplusdiritto.ilsole24ore.com/art/il-regime-pilota-le-infrastrutture-mercato-basate-blockchain-e-altre-dlt-segnale-il-settore-finanziario-europeo-AEMHH4lB

Diario Social. (8 de septiembre, 2023). Aumenta el interés por las criptomonedas y blockchain en República Dominicana, según informe de Sherlock Communications. *Diario Social*. https://diariosocialrd.com/aumenta-el-interes-por-las-criptomonedas-y-blockchain-en-republica-dominicana-segun-informe-de-sherlock-communications/

Directivos y Gerentes. (4 de abril, 2019). Posibilidades del blockchain en la administración pública. *Directivos y Gerentes*. https://directivosygerentes.es/innovacion/noticias-innovacion/posibilidades-blockchain-administracion-publica

El Día. (13 de septiembre, 2023). Criptomonedas y blockchain en RD. *El Día*. https://eldia.com.do/criptomonedas-y-blockchain-en-rd/

Franco, P. (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*. Wiley.

García Valdecasas, P. (27 de mayo, 2022). Blockchain y administración pública. *Tribuna de Opinión Administración Pública Digital*. https://www.administracionpublicadigital.es/tribuna-de-opinion/2022/05/blockchain-y-administracion-publica

Gobierno de Colombia. (2023). *Plan Nacional De Desarrollo 2022-2026*. https://colaboracion.dnp.gov.co/CDT/Prensa/Publicaciones/plan-nacional-de-desarrollo-2022-2026-colombia-potencia-mundial-de-la-vida.pdf

Gobierno de Colombia. (3 de junio, 2023). *Ministerio TIC avanza con el uso e implementación de tecnología Blockchain*. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276398:Ministerio-TIC-avanza-con-el-uso-e-implementacion-de-tecnologia-Blockchain

Gobierno de República Dominicana. (2022). *Plan de Acción 2021-2024 de la Agenda Digital 2030*. https://agendadigital.gob.do/wp-content/uploads/2022/02/Plan-de-Accion-2021-2024-v2.pdf

Guida, G., Messina, A. (21 de octubre, 2020). Blockchain e smart contract: benefici e limiti. *Altalex*. https://www.altalex.com/documents/news/2020/10/21/blockchain-smart-contract-benefici-limiti

Guillén, M. C. (1 de julio, 2022). El uso de criptomonedas aumenta en República Dominicana. *Diario Libre*. https://www.diariolibre.com/economia/finanzas/2022/07/01/el-uso-de-criptomonedas-aumenta-en-republica-dominicana/1921972

Martínez-Pina, A. (7 de abril, 2022). El sandbox europeo: régimen piloto de infraestructuras de mercado basadas en DLT. *Gómez-Acebo & Pombo*. https://www.ga-p.com/publicaciones/el-sandbox-europeo-regimen-piloto-de-infraestructuras-de-mercado-basadas-en-dlt/

Massimo, G. (2018). La *blockchain* e gli smart contracts nell'innovazione del diritto del terzo millennio. *Il diritto dell'informazione e dell'informatica*, 6/2018, 989-1039.

Palá Laguna, R. (8 de junio, 2022). Publicado el Reglamento sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado. *Gómez-Acebo & Pombo*. https://www.ga-p.com/publicaciones/publicado-el-reglamento-sobre-un-regimen-piloto-de-infraestructuras-del-mercado-basadas-en-la-tecnologia-de-registro-descentralizado/

Pastorino, C. (13 de mayo, 2022). Blockchain: qué es y cómo funciona esta tecnología. *Welivesecurity*. https://www.welivesecurity.com/la-es/2022/05/13/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

Portafolio. (21 de junio, 2023). En piloto 'blockchain' para sistemas de alto valor estará el Emisor. *Portafolio*. https://www.portafolio.co/negocios/empresas/ripple-anuncio-colaboracion-con-el-banco-de-la-republica-para-explorar-casos-que-utilicen-la-tecnologia-blockchain-584697

Presidencia de República Dominicana. (2022). *La ciberseguridad en la República Dominicana 2021*. Centro Nacional de Ciberseguridad. https://cncs.gob.do/wp-content/uploads/2022/01/La-Ciberseguridad-en-la-Repu%CC%81blica-Dominicana-2021.pdf

RDo Coin. (15 de julio, 2018). El principio de un ecosistema blockchain en República Dominicana. *Medium*. https://medium.com/@rdo.coin/rdo-coin-el-principio-de-un-ecosistema-blockchain-en-rep%C3%BAblica-dominicana-5f8a87a54ae0

Rinaldi, G. (2019). *Smart contract: meccanizzazione del contratto nel paradigma della blockchain*.

Rodríguez, N. (13 de septiembre, 2020). Más de 20 usos de la tecnología blockchain que debes conocer. *101 Blockchains*. https://101blockchains.com/es/usos-de-la-tecnologia-blockchain/

Sanabria Rátiva, J. A. (8 de mayo, 2023). Tecnologías de la Información y Comunicaciones en el Plan Nacional de Desarrollo. *Blog Jurídico-Tech*. https://telecomunicaciones.uexternado.edu.co/tecnologias-de-la-informacion-y-comunicaciones-en-el-plan-nacional-de-desarrollo/

Sarzana di S. Ippolito, F. (14 de enero, 2019). Blockchain nel Ddl Semplificazioni, conseguenze e problemi dell'attuale testo. *Agenda Digitale*. https://www.agendadigitale.eu/documenti/blockchain-nel-ddl-semplificazioni-conseguenze-e-problemi-dellattuale-testo/

Schmitz, P. E. (26 de abril, 2023). The largest EUPL licensed project? A look to the European *Blockchain* Services Infrastructure (EBSI). *Interoperable Europe Portal*. https://joinup.ec.europa.eu/collection/eupl/news/largest-eupl-licensed-project.

Zona Voz. (23 de febrero, 2024). Desvelando la influencia de la tecnología blockchain en el panorama financiero de la República Dominicana. *Zona Voz RD*. https://zonavoz.com/desvelando-la-influencia-de-la-tecnologia-blockchain-en-el-panorama-financiero-de-la-republica-dominicana/finanzas-personales/

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 155-163

# ¿SON LOS CRIPTOACTIVOS DINERO Y QUÉ IMPLICACIONES TIENEN PARA EL PROYECTO ÁGORA?

*ARE CRYPTO ASSETS MONEY, AND WHICH IMPLICATIONS DO THEY HAVE ON THE AGORA PROJECT?*

**Israel Cedillo Lazcano**

Director de Investigación y Posgrado, Universidad de Las Américas

## Resumen

Desde la introducción de la primera generación de «criptoactivos» representados de forma célebre por Bitcoin, hemos presenciado un proceso de difusión tecnológica que nos ha permitido incorporar a las tecnologías de registro distribuido en diversas áreas de nuestros sistemas financieros e incluso fuera de este. En el contexto de la industria financiera se ha argumentado que ciertos proyectos y aplicaciones representan una revolución que permitirá generar alternativas al sistema financiero regulado e incluso que podría llegar a desplazarlo por completo. Sin embargo, el fenómeno de difusión que atestiguamos no representa algo revolucionario ni novedoso. Históricamente la industria financiera ha adoptado las tecnologías emergentes para mejorar y actualizar sus infraestructuras y en nuestro tiempo esto no es la excepción y como ejemplo de lo anterior podemos mencionar, para el caso mexicano, el proyecto Ágora. Dicho proyecto, coordinado por el Bank for International Settlements (BIS) y en el que participa el Banco de México, no es un proyecto para emitir una Central Bank Digital Currency (CBDC) ni para iniciar el reconocimiento de otros activos en el mercado. Es un proyecto que busca verificar, en armonía con otros similares desarrollados alrededor del mundo, el potencial de *blockchain* para materializar pagos transfronterizos en ejercicio de la *lex monetae*. ¿Se empleará dinero para tal efecto? Ciertamente, pero no en la forma tradicional que se tiene en mente. Para entender lo anterior, a través del presente se busca plantear las diferentes expresiones dinerarias que encontramos en nuestras economías con la finalidad de entender qué es el dinero desde la perspectiva jurídica y así entender el rol de la infraestructura de soporte para su circulación y evolución tomando como ejemplo el caso del Wisselbank del siglo XVII y extrapolando las lecciones obtenidas en el siglo XXI.



## Palabras clave

CBDC, sistemas de pago, criptoactivos, dinero, moneda.



## Abstract

Since the introduction of the first generation of cryptoassets, commonly associated to Bitcoin, we have witnessed a process of technological diffusion that has allowed us to incorporate distributed ledger technologies (DLTs) in different areas within and outside of our financial systems. In the context of the financial industry, it has been argued that certain projects and applications represent a revolution that will foster the emergence of alternative solutions to the regulated financial system, which some argue could even displace it completely. However, the current stage does not represent something revolutionary nor novel. Historically, the financial industry has adopted emergent technologies to improve and update their infrastructures, and, in our context, this trend prevails, as one can verify, in the Mexican context, through the project Agora. The project, which is coordinated by the Bank for International Settlements (BIS) and in which the Bank of Mexico is involved, is not a project designed to issue a Central Bank Digital Currency (CBDC) nor to start recognizing other assets in the market. Agora is a project that seeks to verify, in harmony with other similar projects, the potential of blockchain to materialize cross-border payments in exercise of

the *lex monetae*. Are they going to use money for that purpose? Certainly, but not in its traditional form. To understand this, this paper presents different monetary expressions that one can find throughout our economies with the aim of understanding what is money from a legal perspective, as well as understand the role played by the infrastructures that support its circulation and evolution, taking examples such as the experience of the Wisselbank in the 17th century, while we extrapolate the lessons obtained in the 21st century.

**Keywords**

CBDCs, payment systems, cryptoassets, money, currency.

## Introducción

El 3 de abril de 2024, el Bank for International Settlements (BIS) anunció que daría inicio a otro proyecto que complementa a los proyectos Aurum, Icebreaker, Helvetia, entre otros, mismos que se han estructurado alrededor de la incorporación de registros distribuidos para materializar diferentes esquemas de compensación y liquidación transfronterizos. El proyecto Ágora, entre cuyos participantes podemos encontrar al Banco de México, tiene como objetivo constituir con el sector privado un registro único que permita tokenizar los depósitos recibidos por los bancos comerciales bajo un modelo de dos pilares y efectuar pagos transfronterizos a través de la incorporación de contratos inteligentes (Bank for International Settlements, 2024). Lo anterior representa un conjunto de esfuerzos interesantes y necesarios que han llevado a la especulación relativa a la adopción formal de los «criptoactivos» independientemente de los modelos de diseño involucrados que van desde el modelo descentralizado introducido por Bitcoin hasta los paradigmas centralizados que definen a las Central Bank Digital Currencies (CBDC) como la libra y el euro digitales.

Cuando uno busca analizar y entender la naturaleza, así como los potenciales usos (disruptivos o no) de estas innovaciones, uno tiene que considerar que el mercado de «criptoactivos» se encuentra definido por su diversidad y creciente complejidad. Es decir, el querer explicar y proponer soluciones con base en las características que definen a un solo activo, es un error. Uno debe aventurarse y verificar la existencia de múltiples protocolos que nos permiten generar no solo activos digitales sino también soluciones como contratos inteligentes, aplicaciones descentralizadas (*DApps*) y modelos de negocio como *Blockchain-as-a-Service* (*BaaS*), entre otros. Como es posible colegir de lo anterior, las tecnologías que pueden categorizarse como registros distribuidos nos ofrecen una amplia gama de oportunidades, pero también una fuente de riesgos que deben ser atendidos. ¿Es Ágora una estrategia de *RegTech* encaminada a ese fin? Por ahora, la respuesta es negativa. Ni representa la materialización de los argumentos que ven a Bitcoin como la moneda de curso legal del futuro ni de la creación y difusión del cripto peso que ha sido anunciado como un objetivo de la presente administración. Por ahora nos encontramos ante el desarrollo de un conjunto infraestructural de soporte que busca verificar los potenciales usos que tecnologías como blockchain pueden presentar a nuestros sistemas de pagos transfronterizos. Dicho lo anterior, y con la finalidad de entender mejor lo planteado por estos proyectos y su relevancia en el ejercicio de la *lex monetae* por parte del Estado, primero debemos preguntarnos: ¿son los criptoactivos dinero? o ¿representan un *corpus mechanicum* para incorporar diversas fuentes de liquidez?

## ¿Qué es dinero?

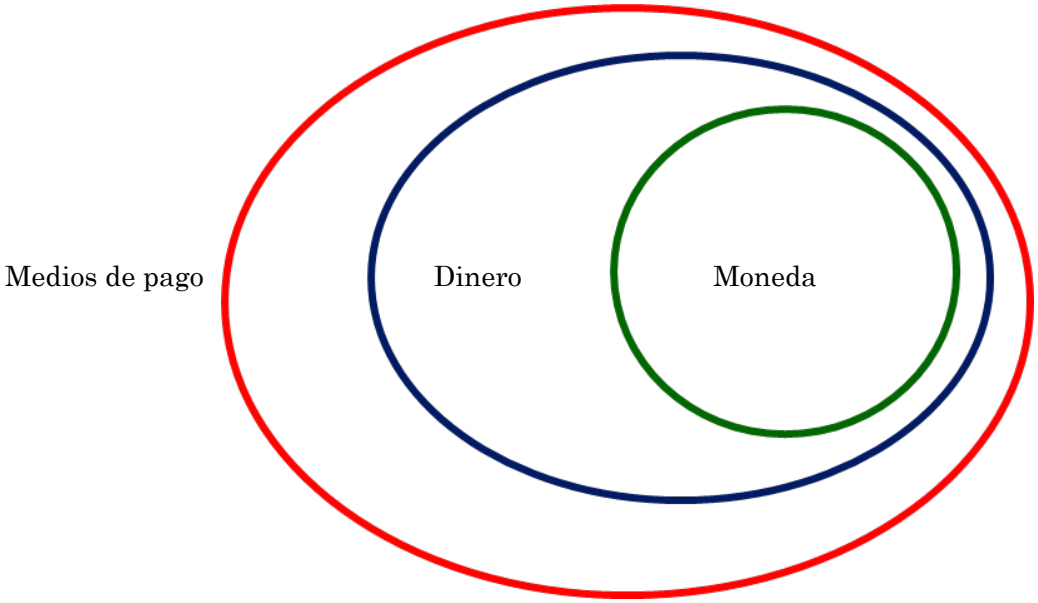
La pregunta aquí presentada se puede percibir, desde un primer punto de vista, como una de diseño y planteamiento simple que puede ser contestada con una respuesta con los mismos elementos cualitativos. Después de todo, al preparar una potencial respuesta, uno puede pensar en diversos símbolos, bienes, sistemas, que son comunes en las interacciones que desarrollamos día a día.

Incluso habrá quienes piensen que la simple mención de una palabra como «pesos», «libras» o «dólares» debería ser más que suficiente para conseguir el fin aquí planteado. Sin embargo, detrás de esta simple pregunta, vamos a toparnos con una gran complejidad de elementos que debemos considerar antes de poder emitir una respuesta que nos permita analizar fenómenos actuales como son el desarrollo y la difusión de diversas categorías de «criptoactivos», incluyendo aquellos que incorporan depósitos siguiendo el modelo de los dineros estables presentadas por Limantour en la transición de los siglos XIX y XX.

Como se puede verificar en el contenido de casos como *Perrin v. Morgan* (Reino Unido, 1943), jueces como Lord Viscount Simon han argumentado sobre la dificultad —si no la imposibilidad— de definir legalmente y de forma estandarizada al dinero, toda vez que la descripción de la realidad jurídica puede variar incluso al interior de una sola jurisdicción. Como ejemplo de lo anterior, el 22 de julio de 2016, en Miami, Florida, la juez Teresa Poole emitió una orden (Estados Unidos de América, 2016, pp. 5-6) en la que adopta una perspectiva funcional clásica para argumentar que dado que los «criptoactivos» no son aceptados por todos los comerciantes ni por todos los proveedores de servicios —haciendo eco al famoso caso británico *Moss v. Hancock* (Reino Unido, 1899)—, aunado a su volatilidad, estos no pueden ser considerados como dinero. Contrastando esta posición, el 19 de septiembre del mismo año, la juez Alison Nathan (Estados Unidos de América, 2015, pp. 5-6) argumentaba con base en la Sección 1960 del *US Code* que dicho ordenamiento no especifica qué es dinero, y solo hace mención a que incluye «fondos». Consecuentemente, Nathan razonó que, dado que estas innovaciones pueden ser consideradas activos líquidos, los cuales pueden ser aceptados como medios de cambio y de pago, estas pueden ser clasificadas como «fondos» y, consecuentemente, como dinero.

Ahora, ciertamente, habrá quien argumente que la definición es muy simple y basta con enlistar las tres funciones tradicionales asociadas al dinero que podemos encontrar en gran parte de las fuentes que existen en la materia: 1) medio de cambio, 2) unidad referencial, y 3) almacén de valor. Sin embargo, desde la perspectiva jurídica, y para atender los fines que nos interesan en el presente, estas simples menciones no son suficientes. Hay que considerar que, en el universo de bienes empleados dentro del comercio, nos encontramos con una gran multiplicidad de activos y pasivos que cumplen con las tres funciones arriba enunciadas. Dicho lo anterior, para dar respuesta a la pregunta aquí planteada, me gusta recurrir el referido caso *Moss v. Hancock*, en el que el juez Darling argumentó que el dinero es todo bien aceptado en el marco de una comunidad para la satisfacción de obligaciones contractuales más allá del círculo y de las características del emisor. Podemos construir sobre la obra de Gurley y Shaw (1960, p. 364) y argumentar que de dicha definición podemos identificar tres categorías de satisfactores contractuales: 1) medios de pago, 2) dinero con fuente de liquidez endógena (dinero), y 3) dinero con fuente de liquidez exógena (moneda):

**Figura 1. Universo de satisfactores contractuales**




Fuente: elaboración propia.

Como se puede colegir de las líneas antes descritas y de la Figura 1, todo activo o pasivo que encontramos en el mercado puede actuar como un medio para satisfacer obligaciones contractuales partiendo del consentimiento en transacciones aisladas (por ejemplo, a través de una permuta, o la adquisición de *commodities* en el sentido planteado por la tesis jurisprudencial *I.3o.C.382 C (10a.)*)[1], hasta la configuración del curso legal como se aprecia en el artículo 8 de la Ley Monetaria de los Estados Unidos Mexicanos.

## 1. Los criptoactivos en el universo dinerario

Con base en lo anterior, y empleando un ejercicio de neutralidad tecnológica, también es posible ubicar a diferentes proyectos de descentralización tecnológica en los diferentes conjuntos que constituyen el universo de satisfactores contractuales que nos ocupan. Por ejemplo, siguiendo el contenido de casos como *AA v. Persons Unknown* (Reino Unido, 2019, p. 28), así como el artículo 30 de la Ley para Regular las Instituciones de Tecnología Financiera (Ley *FinTech*)[2], pode-

1 Transferencias electrónicas interbancarias realizadas desde cuentas en moneda extranjera con destino a cuentas en moneda nacional. Para calcular el tipo de cambio resulta inaplicable lo dispuesto en el primer párrafo del artículo 8 de la Ley Monetaria de los Estados Unidos Mexicanos y debe estarse a lo dispuesto en su tercer párrafo.

2 Artículo 30: «Para efectos de la presente Ley, se considera activo virtual la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas».

mos ubicar a activos como Bitcoin en el marco del conjunto de medios de pago, mientras que el desarrollo de CBDC soportadas por el andamiaje normativo y tecnológico del Estado son un ejemplo de una moneda virtual. Ahora, independientemente de su lugar en el esquema presentado en la Figura 1, debemos entender que, en el contexto de la contratación tradicional, los elementos dinerarios y medios de pago pueden ser considerados como elementos integrales y referenciales de los contratos, existiendo de forma complementaria e independiente al contrato donde se invocan. En el marco de los ecosistemas descentralizados soportados por tecnologías como blockchain, la mayoría de los activos que se encuentran en los conjuntos «dinero» y «moneda» requieren de la interacción entre *smart contracts* (código fuente) y *smart legal contracts* (una forma de contrato digital) para existir y cumplir sus funciones. Es decir, en contextos *on-chain*, los dineros y monedas que se encuentran circulando en estos ecosistemas están estrechamente relacionados con sus respectivos contratos de forma operacional, lo cual nos lleva a colegir que tenemos ante nosotros la base para la constitución de los sistemas de pago del futuro, los cuales no van a depender de instrumentos aislados e independientes, sino de todo un conjunto de componentes que van a jugar un rol activo en la emisión de la orden de pago, el proceso de compensación y la liquidación de la orden, un potencial que diversas entidades públicas y privadas empiezan a explorar.

## Del Amsterdamsche Wisselbank al proyecto Ágora

Los sistemas de pago generalmente son percibidos como mecanismos que permiten a usuarios individuales poner en circulación ciertos activos y pasivos para que estos últimos puedan cumplir con las obligaciones contractuales de quien los emplea. Lo anterior suena simple, pero no carece de sus propias complejidades. De forma análoga, frente a un escenario similar al que estamos atestiguando en el mundo de las finanzas descentralizadas, en el siglo XVII encontramos el caso de un afamado proto banco central en los Países Bajos conocido como el Amsterdamsche Wisselbank. El Wisselbank fue constituido para hacer frente a un problema muy particular: el volumen y la diversidad dineraria. En los mercados de la Europa del siglo XVII, era posible encontrar y transaccionar con cientos, sino miles, de diferentes medios de pago y dineros cuya fuente de liquidez carecía de estandarización. Lo anterior ponía obstáculos al comercio ya que las partes involucradas desconfiaban del medio de pago presentado y se regresaba a un escenario similar al planteado bajo el modelo que define al problema del doble interés empleado para justificar la hipótesis del trueque. Ante dicha situación, el Wisselbank introdujo al mercado un florín bancario estandarizado que actuaba como un primitivo *stablecoin* emitido contra el depósito de ciertos activos para así dar respuesta al problema de estabilidad y de asimetrías cualitativas.

Desafortunadamente, al estar este sistema basado en un modelo en donde los comerciantes podían acceder directamente a la hoja de balance del proto banco central, ante la incertidumbre creada principalmente por la guerra con Inglaterra, los depositantes decidieron retirar de forma masiva el metálico custodiado

por el Wisselbank, ejerciendo los derechos que el *stablecoin* les otorgaba, dejando así al banco sin liquidez para cumplir con obligaciones a largo plazo y sostener su propia existencia (Frost, Shin y Wierts, 2020). Ante experiencias como la aquí planteada, cuando se habla de diseñar un modelo para el mundo financiero de la cuarta revolución industrial, se ha discutido entre dos modelos: 1) el denominado de un pilar que da acceso directo a los usuarios a nodos asociados a la cadena de bloques y balances del banco central; y 2) otro que depende de la existencia de intermediarios regulados quienes tienen acceso a la cadena y a la hoja de balance controladas por el banco central, mientras que ofertan soluciones *off-chain* para los usuarios. Cuando uno lee los reportes de proyectos como la *e-krona* sueca y la libra digital del Reino Unido, podemos anticipar que un diseño para el peso digital se centrará en un modelo de dos pilares, argumento que se puede verificar en la convocatoria que ha emitido el banco central para que bancos comerciales actúen como elementos nodales del proyecto Ágora.

## Preparando el futuro en el Ágora

Cuando uno lee los elementos constitutivos del proyecto Ágora, nos encontramos con un modelo interesante. En contraste con el modelo desplegado en el pasado por el Wisselbank, que podría denominarse de un pilar, Ágora se estructura alrededor de dos pilares en donde encontramos una red de convenios entre bancos corresponsables constituidos en diversas jurisdicciones que compensan y liquidan transacciones iniciadas por sus clientes y contrapartes asociados a diferentes bancos. Bajo este proyecto el modelo se mantendrá en gran medida sin cambios. Es decir, Ágora depende de un esquema de tokenización similar al empleado por el Wisselbank en el pasado y actualmente empleado para crear *stablecoins* en cadenas de bloques, con la variación de que el proceso en la cadena va a ser empleado para incorporar liquidez exógena, en otras palabras, se tokenizarán los elementos que corresponden al agregado monetario M1.

Los nodos dentro de la cadena que complementan al nodo emisor del banco central estarán asignados a los bancos comerciales seleccionados quienes, con base en las características antes referidas de los smart contracts más los requerimientos de establecidos en estándares como la ISO 20022, podrán combinar la mensajería asociada a los pagos con los ajustes en sus *ledgers* respectivos reflejando de forma automatizada los procesos de compensación y liquidación, a la vez que podrán uniformar los requerimientos solicitados a los clientes *off-chain* relativos a la creación de identidades digitales para cumplimiento de la normatividad en materia de lavado de dinero y financiamiento al terrorismo.

## Conclusiones

Como el lector puede apreciar, a pesar de que Ágora no se centra en la emisión al público de una CBDC, sí permitirá asentar las bases para los sistemas de pagos del futuro. Uno podrá argumentar que, por el momento, el proyecto se centra en el tratamiento de transacciones de alto volumen; sin embargo, los elementos constitutivos que van desde la tokenización de moneda hasta las

diferenciales de privacidad bajo un ID único dentro de una cadena bien definida y regulada permitirá en el corto y mediano plazo anticipar como lucirán los sistemas de pago basados en registros distribuidos que soportarán al peso digital y que lo harán interoperable con los sistemas que sostendrán a otras CBDC alrededor del mundo. Asimismo, en esta etapa, los participantes en Ágora podrán familiarizarse con los proveedores e implementadores de la tecnología involucrada para poder iniciar con los mapeos requeridos en materia de resiliencia operacional y así desplegar, en su momento, sistemas de pagos más seguros que incrementarán la confianza al interior de un mercado caracterizado por sus bajos niveles de bancarización.

## Referencias bibliográficas

Bank for International Settlements. (2024). Project Agorá moves to next phase and opens up call for private sector participation. *BIS*. https://www.bis.org/about/bisih/topics/fmis/agora.htm

Estados Unidos de América. (2014). *The State of Florida v Michelle Abner Espinoza, F14-2923 FL (US).*

Estados Unidos de América. (2015). *U.S. v Murgio et al., 15-cr-00769 AJN (US).*

Frost, J., Shin, H. S., Wierts, P. (2020). An early stablecoin? The Bank of Amsterdam and the governance of money. *BIS*. https://www.bis.org/publ/work902.pdf

Gurley, J. G., Shaw, E. S. (1960). *Money in a Theory of Finance*. The Brookings Institution.

Reino Unido. (1899). *Moss v Hancock, 2 Q.B. 111 (UK).*

Reino Unido. (1943). *Perrin v Morgan, A.C. 399 HL (UK).*

Reino Unido. (2019). *AA v Persons Unknown EWHC 3556 (Comm) (UK).*

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 165-176

# ESTRATEGIA NACIONAL DE INTELIGENCIA ARTIFICIAL DE LA REPÚBLICA DOMINICANA: DESAFÍOS Y REGULACIÓN EN PROTECCIÓN DE DATOS

*DOMINICAN REPUBLIC'S NATIONAL ARTIFICIAL INTELLIGENCE STRATEGY: CHALLENGES AND REGULATION IN DATA PROTECTION*

**Félix Juan Rivera**

Letrado del Gabinete Técnico de la Suprema Corte de Justicia

## Resumen

La República Dominicana presentó en octubre de 2023 su Estrategia Nacional de Inteligencia Artificial (ENIA) con el objetivo de modernizar los servicios públicos y fomentar la eficiencia del Estado mediante la IA. Esta iniciativa busca no solo la automatización de procesos y la creación de aplicaciones personalizadas, sino también convertir al país en un referente regional en IA. Sin embargo, la implementación de la IA presenta varios desafíos, especialmente en términos de protección de datos, privacidad, igualdad y no discriminación. La investigación aborda estos retos, tomando como referencia el Reglamento General de Protección de Datos (RGPD) de la UE, y analiza cómo la ENIA propone modificar la Ley 172-13 para fortalecer el marco legal de protección de datos. Se destacan las complejidades del consentimiento informado, la gestión del tiempo de almacenamiento de datos, el derecho de supresión, y la elaboración de perfiles y decisiones automatizadas. La investigación subraya la necesidad de equilibrar la innovación tecnológica con la protección de los derechos humanos y propone medidas específicas para garantizar la privacidad y la transparencia en el uso de la IA.



## Palabras clave

Inteligencia artificial, protección de datos, ENIA, regulación, privacidad.



## Abstract

In October 2023, the Dominican Republic introduced its National Artificial Intelligence Strategy (ENIA) aimed at modernizing public services and enhancing state efficiency through AI. This initiative seeks not only to automate processes and develop customized applications, but also to establish the country as a regional leader in AI. However, AI implementation presents several challenges, particularly concerning data protection, privacy, equality, and non-discrimination. The research addresses these challenges, drawing on the European Union's General Data Protection Regulation (GDPR), and analyzes how ENIA proposes amendments to strengthen the legal framework under Law No. 172-13 for data protection. The complexities of informed consent, data retention management, the right to erasure, and profiling and automated decision-making are highlighted. The research underscores the need to balance technological innovation with the protection of human rights and proposes specific measures to ensure privacy and transparency in AI usage.



## Keywords

Artificial intelligence, data protection, ENIA, regulation, privacy.

## Introducción

La República Dominicana, siguiendo el impulso de la era digital, así como la necesidad de modernización, en octubre de 2023 presentó la Estrategia Nacional de Inteligencia Artificial (en adelante, ENIA). La reciente iniciativa ha sido liderada por el Gabinete de Innovación y Desarrollo Digital y la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) de la Presidencia de la República, con el objetivo de que la ENIA constituya una herramienta crucial para la automatización de los servicios públicos, la creación de aplicaciones personalizadas y el desarrollo de *software* que fortalezcan la eficiencia del Estado.

La inteligencia artificial (en adelante, IA) constituye el eje esencial de esta estrategia, pues ha sido un fenómeno tecnológico con el potencial de mejorar las organizaciones e instituciones del Estado, no solo en su gestión y procesos internos, sino también en los nuevos modelos de negocios, productos y servicios. Asimismo, representa un gran avance para la administración pública en cuanto a las decisiones administrativas o jurisdiccionales, así como también en los sistemas objetivos de selección de empleados públicos o incremento en la protección policial.

No obstante su implementación, la IA no está exenta de desafíos, ya que a pesar de sus ventajas significativas produce efectos negativos, debido a que afecta derechos individuales, especialmente la protección de datos, la intimidad, la igualdad y la no discriminación. Es más, puede provocar la desaparición de puestos de trabajos o incrementar la discriminación por diferentes circunstancias.

La ENIA, alineada a los principios éticos de la Unesco, persigue transformar a la República Dominicana en un referente regional en materia de IA, manteniendo el equilibrio entre la innovación tecnológica y la preservación de los valores fundamentales de los derechos humanos. La estrategia aborda cuatro pilares claves que se enuncian a continuación: gobierno inteligente, *hub* de talento humano e innovación, *hub* de datos y escala regional.

En la presente investigación analizaremos los retos y desafíos que tiene la República Dominicana en la actualización y regulación del marco normativo frente a la privacidad y la protección de los datos en el contexto de la IA generativa. Como afirma Barrio Andrés (2024), hemos pasado de la simple regulación ética a la regulación jurídica, y es por ello que tomaremos como referencia el Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 (RGPD), haciendo énfasis en aspectos como el consentimiento informado, el tiempo de almacenamiento de los datos, el derecho de supresión, la elaboración de perfiles y las decisiones automatizadas.

## Estrategia Nacional de Inteligencia Artificial (ENIA)

Como señala el Gabinete de Innovación y Desarrollo Digital y la Oficina Gubernamental de Tecnologías de la Información y Comunicación (2023), la ENIA es una herramienta de tecnología exponencial para automatizar los servicios ciudadanos, acercándose a una educación personalizada y crear en el país

aplicaciones y *softwares* que conecten a la sociedad dominicana con un Estado más eficiente.

La IA es un término difícil de conceptualizar puesto que abarca un conjunto de tecnologías que comprende desde aprendizaje automático con uso de grandes volúmenes de datos, hasta lógica de deducción basada en modelos.

No obstante ello, la ENIA adopta el concepto de IA que recoge el instrumento normativo sobre ética de la inteligencia artificial de la Unesco de noviembre de 2021, en el cual se define como las tecnologías de procesamiento de la información que integran modelos y algoritmos que producen una capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como la predicción y la adopción de decisiones en entornos materiales y virtuales. Los sistemas de IA están diseñados para funcionar con diferentes grados de autonomía, mediante la modelización y representación del conocimiento y la explotación de datos y el cálculo de correlaciones (OGTIC, 2023, p. 17).

En ese orden, la ENIA tiene por finalidad que la República Dominicana se convierta en un referente regional de la IA, al tiempo que se salvaguarden los valores fundamentales de los derechos humanos y la democracia (OGTIC, 2023, p. 19). Para ello, la ENIA delimitó cuatro pilares, que fungen como objetivos para lograr la correcta implementación de la innovadora iniciativa. En ese sentido, a continuación, lo enunciamos brevemente y a su vez indicamos el propósito de cada uno:

- Gobierno inteligente: prioriza la gobernanza de la IA a través de políticas públicas y robustece el marco normativo para el uso ético en el sector público.
- *Hub* de talento humano e innovación: reúne a diversos actores, como investigadores, empresas, ONG y agencias gubernamentales, formando una coalición para crear un ecosistema de innovación dinámico, promoviendo tecnologías avanzadas, la colaboración abierta y la integración regional.
- *Hub* de datos: pretende impulsar una infraestructura tecnológica avanzada para procesar, almacenar y analizar datos en inteligencia artificial.
- Escala regional: transversal a los otros pilares enfocado en potenciar y expandir el alcance del *hub* de talento humano e innovación a nivel regional mediante asociaciones con el sector privado, la academia y la sociedad civil en Centroamérica, el Caribe y Latinoamérica.

En el primer pilar, denominado «gobierno inteligente», la privacidad se concibe como uno de los grandes desafíos, debido a la IA generativa, como son los transformadores preentrenados generativos (GPT, por sus siglas en inglés). Esta tecnología ofrece nuevas formas de automatización, optimización de procesos y toma de decisiones, lo que puede impulsar la productividad y generar impactos significativos en diferentes sectores económicos (OGTIC, 2023, p. 18). Los debates sobre cuestiones como el impacto en nuestras vidas de la pérdida de control sobre nuestros datos solo se intensificarán en los próximos años (OGTIC, 2023, p. 18).

Ante la situación enunciada, el primer pilar asumió como objetivo 1.2 la necesidad de impulsar una adopción ética y responsable de la IA en República

Dominicana y, a su vez, fortalecer el marco legal y regulatorio de protección de datos. Cabe preguntarse, ¿cómo pretende la ENIA alcanzar el objetivo expuesto? Para ello, la estrategia trazó diversas medidas, que se describen en las próximas líneas.

1. Se aspira a modificar la Ley 172-13 sobre la Protección Integral de los Datos Personales, a fin de establecer salvaguardas fundamentales para garantizar la protección de la privacidad y los derechos humanos en el contexto de la IA (OGTIC, 2023, p. 37), incluyendo una serie de medidas orientadas no solo a aspectos como la recopilación, uso y almacenamiento de los datos, sino también a la ética, privacidad, protección de datos, responsabilidad y transparencia en el uso de la IA.
2. Se busca fortalecer el control de los usuarios sobre sus datos personales estableciendo los derechos de acceder, modificar, limitar o borrar los datos, brindando un mayor grado de autonomía y empoderamiento sobre su información (OGTIC, 2023, p. 38). Sin embargo, la Ley 172-13, antes citada, alude a estos derechos en sus artículos 7 y 8, relativos a la acción de *habeas data* y a las condiciones en sentido general para el ejercicio de los derechos a proteger.
3. Se pretende establecer un marco de notificaciones y de cómo se deberá recoger el consentimiento, especificando en qué caso y bajo qué condiciones serán tratados los datos personales. Según la estrategia esto permitirá que los individuos estén plenamente advertidos sobre cómo se utilizarán sus datos y puedan ejercer un consentimiento informado y libre (OGTIC, 2023, p. 38).
4. Se procura fortalecer los principios como requisitos de transparencia para los responsables del tratamiento, garantizando que se brinde información clara y comprensible sobre cómo se utilizan los datos y con qué fines, así como requisitos específicos como la minimización de los datos, para incentivar al responsable del tratamiento a recolectar los datos estrictamente necesarios y relevantes de acuerdo al fin perseguido con la IA.
5. En cuanto a los datos sensibles que se definen conceptualmente como aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual (Ley 172-13, art. 6) recibirán una atención especial en lo relativo a su protección asegurando su confidencialidad y respeto a la privacidad del titular.
6. Finalmente, se creará una entidad administrativa responsable no solo de supervisar y garantizar el cumplimiento de las normas de protección de datos, sino también, de brindar asesoría y orientación en la materia.

Ahora bien, para que exista una correcta aplicación y efectivo cumplimiento de la autoridad de control, se debe instaurar, naturalmente, mecanismos de indemnización para sancionar a las organizaciones responsables del tratamiento que hagan un uso ilegítimo de los datos personales.

## Estado del arte de la inteligencia artificial

En las últimas décadas la IA ha experimentado avances sustanciales transformando todos los sectores de la sociedad generando grandes desafíos éticos y legales por su continua evolución y desarrollo. En este apartado, nos centraremos en el estado del arte de la IA focalizado especialmente en las implicaciones para la intimidad y la protección de datos de las personas.

Hemos visto cómo las grandes empresas dedicadas al desarrollo de tecnología han logrado avances en técnicas de aprendizaje automático, como lo es el aprendizaje profundo. Los algoritmos de aprendizaje automático basados en redes neuronales profundas han logrado un rendimiento superior en tareas como el reconocimiento de imágenes, el procesamiento del lenguaje natural y el juego de estrategia (OAS Youth Academy, 2023, p. 4).

### 1. Evolución de la inteligencia artificial generativa

Podemos afirmar que la evolución de la técnica de la IA abarca desde redes neuronales hasta los modelos de aprendizaje profundo. Gracias a modelos como GPT-4 de OpenAI, Bard de Google o Bing Chat de Microsoft, hemos alcanzado niveles de realismo profundo en la generación de texto, imágenes y videos.

GPT-4 de OpenAI es un modelo capacitado para seguir una instrucción en un mensaje y proporcionar una respuesta detallada. Este modelo ha sido entrenado gracias al aprendizaje por refuerzo partiendo desde la retroalimentación humana, pero con ligera diferencia en la configuración de recopilación de datos. Sin embargo, hay un sinnúmero de limitaciones que presenta este modelo, como pueden ser respuestas que suenan plausibles pero incorrectas o sin sentido, afirmar que no sabe la respuesta, pero si la reformula, puede responder correctamente, responde a instrucciones dañinas o mostrará un comportamiento sesgado, entre otros.

Bard de Google es una nueva herramienta que puedes usar para descubrir ideas creativas y explicar cuestiones de forma sencilla. Es un experimento de la IA de Google que puede generar texto, traducir idiomas, escribir diferentes tipos de contenido creativo y más. Este modelo formula respuestas utilizando los datos que ya conoce y que obtiene de otras fuentes proporcionadas por otros servicios de Google.

A pesar de ello, Google reconoce que este modelo puede proporcionar información inexacta o hacer afirmaciones ofensivas y es el usuario el que debe de verificar la información que proporciona la aplicación marcando las respuestas como correctas o incorrectas, incluso se tiene la posibilidad de denunciar algún problema legal cuando corresponda.

Bing Chat de Microsoft fue renombrado como Microsoft Copilot a partir del 15 de noviembre de 2023. La herramienta consiste, básicamente, en tener un asistente de investigación, un planificador personal y un socio creativo a su lado cada vez que realiza una búsqueda en la web. Con este conjunto de funciones se puede obtener respuestas detalladas, ser creativo escribiendo poemas, historias e incluso crear imágenes completamente nuevas.

No obstante a lo anterior, el usuario de este servicio no solo puede obtener resultados inesperados con temas potencialmente dañinos, sino que también, en ocasiones, tergiversará la información y es posible que la respuesta parezca convincente, pero está incompleta, inexacta o inapropiada.

## 2. Aplicaciones de la inteligencia artificial

Algunas de las aplicaciones que más se han destacado en todo el desarrollo de la IA son las siguientes (OAS Youth Academy, 2023, p. 7):

- Asistentes virtuales: los asistentes virtuales y *chatbots* utilizan técnicas de procesamiento del lenguaje natural para comprender y responder a las preguntas y solicitudes de los usuarios.
- Reconocimiento de imágenes y video: los algoritmos de visión por computadora permiten a las maquinas identificar y clasificar objetos y patrones en imágenes y videos.
- Aprendizaje automático: el aprendizaje automático permite a las máquinas aprender a partir de los datos, sin necesidad de ser programadas explícitamente.
- Robótica: la robótica se utiliza en aplicaciones como la manufactura, la exploración espacial, la atención médica y la agricultura.
- Diagnóstico y tratamiento médico: la inteligencia artificial se utiliza en el diagnóstico médico, el diseño de tratamientos personalizados y el monitoreo de la salud.
- Optimización empresarial: la inteligencia artificial se utiliza en la optimización de procesos empresariales, como la planificación de la cadena de suministro, la predicción de la demanda y la detección de fraudes.

A pesar de los avances significativos mencionados precedentemente, hay que reconocer que en el campo de la IA todavía hay tareas pendientes por resolver, verbigracia, la seguridad y fiabilidad de los sistemas, la justicia y la imparcialidad de los modelos y el desarrollo de aplicaciones que puedan entender y razonar similar a los humanos constituyen algunos problemas que deben ser solucionados en un futuro no muy lejano, por la importancia que representa para las personas.

## Retos y desafíos

Los grandes modelos lingüísticos (LLM, por las siglas inglesas de *large language models*), como pueden ser GPT-4 de OpenAI, Bard de Google o Bing Chat de Microsoft, le han dado un giro al procesamiento del lenguaje natural enfrentando múltiples desafíos contra la intimidad y la protección de los datos. El funcionamiento de esta rama de la IA opera con grandes recopilaciones de datos para entrenar estos modelos, lo que plantea una serie de cuestionamientos respecto al consentimiento informado y explícito del usuario, el tiempo de almacenamiento o la supresión de los datos, la elaboración de perfiles y las decisiones automatizadas.

Es por ello, que surge la necesidad de equilibrar la innovación de dicha tecnología con la tutela de la privacidad lo que supone un dilema constante para los desarrolladores de IA y las instituciones facultadas para regular lo enunciado.

En los procesos donde existe tratamiento de datos personales se debe cumplir con las normas relativas a la protección de datos. En ese sentido, la República Dominicana ha iniciado a través de la ENIA con la adaptación y actualización del marco regulatorio, en tanto tomaremos como parámetro el Reglamento General de Protección de Datos, que es el instrumento internacional de referencia, para señalar algunos de los retos y desafíos que deberán afrontar las autoridades nacionales para dar respuesta a los problemas que se generan frente al tratamiento de los datos personales mediante el uso de la IA.

## 1. Consentimiento informado y explícito del usuario

El funcionamiento de la IA es posible gracias al entrenamiento de un conjunto de grandes volúmenes de datos de diversas fuentes, lo que supone que el proceso de consentimiento en las interacciones con los principales LLM resulta ambiguo, ya que los usuarios no siempre son plenamente conscientes de cómo se utilizan sus datos (Barrio Andrés, 2023), pues no se informa correctamente al titular de cómo sus datos ayudan a la formación y ejecución de la IA.

En ese orden, supone un desafío cumplir con el requisito que exige el RGPD en el sentido de que el consentimiento sea informado y explícito, es decir, debemos de entender que el titular de los datos cuenta con un poder de disposición sobre sus propios datos personales, pudiendo decidir sobre su uso y destino. Así lo señala la sentencia del Tribunal Constitucional n.º 292/2000 del 30 de noviembre que, dentro de sus fundamentos jurídicos, establece que ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

El propio RGPD traza las condiciones que se deben configurar para recabar el consentimiento de manera adecuada. Estas condiciones son las siguientes: por separado, de manera inequívoca y afirmativa, granular, normativo, demostrable, documentado y revocable. En ese orden de ideas, el consentimiento le otorga la posibilidad al titular de tener libertad y control sobre sus datos personales, ya que si no se tiene la libertad para elegir o si se exige el consentimiento para fines de un tratamiento que no está relacionado con el servicio que se presta, pues no puede considerarse un consentimiento ni libre ni válido.

En consecuencia, los datos tratados en estos modelos son de fuentes diversas, lo que hace difícil informar a los titulares de manera precisa sobre cómo se utilizan, quiénes lo poseen y con qué fin. Además, modelos como GPT-4, por su propia naturaleza, tienen una complejidad intrínseca que dificulta explicar detalladamente la finalidad para la cual se utilizan los datos, siendo un requisito esencial del RGPD; y por último, los sesgos que pueden dar lugar a discriminación, esto genera dificultad para garantizar el consentimiento informado, puesto que los titulares de los datos no comprenderían plenamente los riesgos ligados al uso del modelo de IA.

## 2. Tiempo de almacenamiento de datos

El literal *e* del artículo 5.1 del RGPD señala que los datos personales deberán ser conservados de tal manera que hagan posible la identificación de los interesados por un tiempo no superior a aquel que resulte imprescindible para el cumplimiento de las finalidades del tratamiento de los datos personales.

El cumplimiento del principio de limitación del plazo de conservación es un tema polémico y sobre todo en el desarrollo de los modelos lingüísticos, en vista de que el almacenamiento de los datos debe ser estrictamente necesario en función del tratamiento para lo cual ha sido solicitado el consentimiento, pero teniendo en cuenta que estos modelos aprenden y mejoran con el tiempo, esto supone la dificultad previa de fijar un plazo determinado para almacenar los datos.

Esto significa que el continuo aprendizaje y la constante evolución de los datos para entrenar a las principales LLM genera dificultades para fijar o establecer dentro de las políticas de seguridad un límite en el plazo de conservación que exige el RGPD. Es importante destacar que el aprendizaje automático supone la retención de datos por un prolongado período de tiempo, lo que dificulta precisar un período de conservación. Ejemplos como los *chatbots* o asistentes virtuales precisan de almacenamiento de datos en tiempo real con la finalidad de ofrecer respuestas y esto representa un obstáculo al momento de establecer un límite rígido respecto al almacenamiento de la información sin que esto afecte la capacidad de ofrecer resultados precisos.

## 3. Supresión de datos

El RGPD en el artículo 17, plantea que el titular tendrá derecho a solicitar la supresión de los datos bajo una serie de circunstancias específicas. Esto supone un problema técnico aún no resuelto, en razón de que nos debemos preguntar: ¿cómo pueden eliminarse datos específicos de un usuario de un modelo que ha sido entrenado con esos datos? (Barrio Andrés, 2023).

Técnicamente existe la complejidad de eliminar datos selectivos a consecuencia de que en el supuesto de que se haya efectuado la eliminación de los datos, el «proceso de olvido» podría no haber culminado, esto porque la información conocida por el modelo pasa a formar parte de su memoria, en consecuencia, posible de ser recordada y empleada pese a haberse eliminado el dato que sirvió de insumo (Niño, 2023).

Esto abre la ventana de la posibilidad de ejercer el derecho al olvido, el cual es definido por la Agencia Española de Protección de Datos (2023) como la manifestación del derecho de supresión aplicado a los buscadores de internet, teniendo procedencia cuando los datos personales expuestos en internet no cumplen con los requisitos de adecuación y pertinencia exigidos por la normativa, lo que produce que se limite la difusión de toda aquella información personal que sea obsoleta o no tenga relevancia ni interés público, aunque siendo negativa, haya sido una publicación legítima.

En consecuencia, las organizaciones que en el desarrollo de sus actividades incorporen modelos de LLM deberán acondicionar en sus procesos la posibilidad

de suprimir datos personales a requerimiento del titular, pero es que los modelos, entre otras cosas, se entrenan con grandes volúmenes de datos, generan textos de manera autónoma, almacenan y distribuyen los datos, lo que hace que el ejercicio de este derecho presente grandes desafíos lógicos y técnicos.

### 4. Elaboración de perfiles y decisiones automatizadas

El artículo 22 del RGPD señala que el titular de los datos tiene derecho a no ser objeto de una decisión basada exclusivamente en el tratamiento automatizado de los datos personales del interesado, incluida la elaboración de perfiles, que produzca determinados efectos jurídicos en el interesado o le repercuta de un modo significativo de manera similar.

La opacidad en la toma de decisiones por parte de los modelos lingüísticos puede resultar contraproducentes debido a que en la forma en que el algoritmo fórmula los perfiles y toma decisión automatizada dificulta su comprensión. La cantidad de obstáculos técnicos que dificultan la explicación de decisiones autónomas basadas en algoritmos depende de la complejidad de estos. Numerosos autores afirman que es casi imposible explicar la lógica que hay tras un algoritmo que adopta una decisión (Brkan, s. f.).

En contraposición a ello, el titular como propietario de sus datos posee el derecho a que se le comunique la lógica que conlleva el tratamiento de sus datos y si se trata de elaboración de perfiles o decisiones automatizadas cuáles serían las consecuencias de dicho tratamiento. Se trata de una exigencia que indudablemente el responsable del tratamiento no estaría en condiciones adecuadas para dar respuesta al presente desafío.

Finalmente, la propia naturaleza compleja de los modelos de IA de generar texto, la capacidad de absorber sesgos inherentes, entre otras funciones, implican grandes retos, puesto que tienen la capacidad de tomar decisiones sobre datos que no fueron proporcionados por los titulares, lo que evidentemente expone la falta de mecanismos explícitos para que los usuarios no sean objetos de elaboración de perfiles y ser expuestos a decisiones automatizadas.

## Conclusiones

En el análisis de la Estrategia Nacional de Inteligencia Artificial de la República Dominicana y sus implicaciones en la protección de datos personales, especialmente en aspectos cruciales como el consentimiento informado, el tiempo de almacenamiento de datos, el derecho de supresión, elaboración de perfiles y decisiones automatizadas, emergen diversos retos y desafíos que requieren atención y soluciones ponderadas.

Hemos visto que el consentimiento informado y explícito del titular de los datos genera una complejidad inherente en los modelos lingüísticos de IA, evidentemente plantea un desafío en la obtención del consentimiento y en el deber de informar al usuario de cuál será la finalidad de los datos. La confusión sobre cómo se utilizarán los datos en el entrenamiento de estos modelos y la dificultad

de explicar la finalidad exacta de su uso genera interrogantes aún no resueltas sobre la validez y libertad del consentimiento.

La evolución continua de los modelos de IA complica el tiempo de almacenamiento de los datos, puesto que la necesidad de almacenar datos a largo plazo para el aprendizaje continuo y la toma de decisión choca con el principio de limitación establecido en el Reglamento General de Protección de Datos.

La dificultad técnica de eliminar datos específicos de un usuario en modelos ya entrenados plantea un reto significativo en el cumplimiento del derecho de supresión. La retención de información en la memoria de los modelos incluso después de la eliminación del dato original complica la posibilidad de ejercer el derecho al olvido.

La poca transparencia en la toma decisiones en los modelos lingüísticos, aunado a la dificultad de explicar la lógica detrás de la elaboración de los perfiles y las decisiones automatizadas, contradice el derecho del titular de los datos a ser informado sobre el procesamiento de sus datos. La complejidad inherente a estos algoritmos dificulta la comprensión y comunicación de tales procesos.

Finalmente, el fortalecimiento y actualización del marco legal, particularmente la modificación de la Ley 172-13, sobre la Protección Integral de los Datos Personales, es esencial para abordar los desafíos emergentes. Asegurar la protección de la intimidad y los derechos humanos en general en el uso de la IA implica ajustar la legislación a las realidades y complejidades actuales que generan estos modelos.

Es por ello que la convergencia de la innovación tecnológica y la protección de datos plantea una serie de dilemas éticos y técnicos que deben abordarse para lograr un equilibrio adecuado entre el avance tecnológico y la salvaguarda de los derechos sobre protección de datos. La República Dominicana, al aspirar a convertirse en un referente regional en IA, encara la responsabilidad de enfrentar estos retos con soluciones innovadoras y éticas que promuevan el desarrollo sostenible y el respeto a los derechos fundamentales.

## Referencias bibliográficas


Barrio Andrés, M. (2024). Retos de la inteligencia artificial ¿Principios éticos o regulación jurídica? *Seminario Escuela de Práctica Jurídica-UCM*. https://www.youtube.com/watch?v=tWA5VNF_QQc&ab_channel=EscueladePr%C3%A1cticaJur%C3%ADdica-UCM

Brkan, M. (s.f.). *Inteligencia artificial, aprendizaje automático, algoritmos y protección de datos en el marco del RGPD y más allá*. Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/142586/2/Entornos%20digitales%20y%20nuevos%20retos%20para%20la%20protecci%C3%B3n%20de%20datos_M%C3%B3dulo%202_%20Inteligencia%20artificial%2C%20aprendizaje%20autom%C3%A1tico%2C%20algoritmos%20y%20protecci%C3%B3n%20de%20datos%20en%20el%20marco%20del%20RGPD%20y%20m%C3%A1s%20all%C3%A1.pdf

OAS Youth Academy. (2023). *Introducción a la inteligencia artificial*.

Oficina Gubernamental de Tecnologías de la Información y Comunicación. (11 de octubre, 2023). *Presidente Luis Abinader lanza la Estrategia Nacional de IA*. https://ogtic.gob.do/presidente-luis-abinader-lanza-la-estrategia-nacional-de-inteligencia-artificial/

Oficina Gubernamental de Tecnologías de la Información y Comunicación. (2023). *Estrategia Nacional de Inteligencia Artificial*. Dirección Ejecutiva del Gabinete de Innovación y Desarrollo Digital. https://ogtic.gob.do/wp-content/uploads/2023/10/ENIA-Estrategia-Nacional-de-Inteligencia-Artificial-de-la-Republica-Dominicana_compressed.pdf

República Dominicana. (2013). *Ley núm. 172-13, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados*. https://biblioteca.enj.org/bitstream/handle/123456789/125418/Ley%20172-13.pdf?sequence=1&isAllowed=y

España. Tribunal Constitucional. (30 de noviembre, 2000). Sentencia 292/2000. *Boletín Oficial del Estado*. https://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf

Niño, H. (17 de octubre, 2023). La IA vs. el Derecho al Olvido ¿Esta inteligencia también tiene la capacidad de olvidar? *Prometheo*. https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/chatgpt-y-proteccion-de-datos/

Agencia Española de Protección de Datos. (10 de noviembre, 2023). *Derecho de supresión ("al olvido"): buscadores de internet*. https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido

Barrio Andrés, M. (13 de noviembre, 2023). ChatGPT y protección de datos. *Abogacía Española*. https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/chatgpt-y-proteccion-de-datos/

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 177-186

# EL COSTO DE ACCEDER A LA SALA POLÍTICO-ADMINISTRATIVA DEL TRIBUNAL SUPREMO DE JUSTICIA EN VENEZUELA Y LA IMPLEMENTACIÓN DE LAS TIC

The cost of accessing the political-administrative chamber of the Supreme Court of Justice in Venezuela and the implementation of ICTs

**Nathaly Vielma**

Estudiante de Derecho, Universidad Central de Venezuela

## Resumen

La Sala Político-Administrativa del Tribunal Supremo de Justicia conoce principalmente de tres procedimientos previstos en la Ley Orgánica de la Jurisdicción Contencioso-Administrativa: el procedimiento de las pretensiones procesales administrativas de contenido patrimonial, el procedimiento breve y el procedimiento común a las pretensiones de nulidad, interpretación y controversia administrativa. Los costos operativos para una persona que no reside en Caracas al iniciar un juicio varían en función de determinar la cantidad de actuaciones que correspondan según el procedimiento respectivo y las veces que tenga que trasladarse a la Sala Político-Administrativa, ya que deben cubrir los costos de transporte, alojamiento, comida, entre otros. Todo ello debido a que las actuaciones deben realizarse necesariamente de forma presencial y por escrito en papel, ello por cuanto no existe a la fecha la implementación de algún plan de desarrollo de las Tecnologías de la Información y la Comunicación (TIC) al servicio del sistema judicial venezolano y sus usuarios.



## Palabras clave

Acceso a la justicia, justicia digital, tutela judicial efectiva, derecho procesal administrativo.



## Abstract

The Political-Administrative Chamber of the Supreme Court of Justice mainly hears three procedures provided for in the Organic Law of the Contentious-Administrative Jurisdiction: the procedure for administrative claims of patrimonial content, the brief procedure and the common procedure for claims for nullity, interpretation and administrative controversy. The operating costs for a person who does not reside in Caracas when starting a trial vary depending on determining the number of actions that correspond according to the respective procedure and the times they have to go to the Political-Administrative Chamber, since they must cover the costs of transportation, accommodation, food, among others. This is due to the fact that the actions must necessarily be carried out in person and in writing on paper, since to date there is no implementation of any development plan for Information and Communication Technologies (ICTs) at the service of the Venezuelan judicial system and its users.



## Keywords

Access to justice, digital justice, effective judicial protection, administrative procedural law.

## Introducción

La Ley Orgánica de la Jurisdicción Contencioso Administrativa[1] prevé tres procedimientos en primera instancia[2] que están regulados en los artículos 56 y siguientes, para tramitar las principales pretensiones que se demanden ante los Juzgados Municipales[3], Juzgados Nacionales[4], Juzgados Superiores Estadales de la Jurisdicción Contencioso-Administrativa[5] y ante la Sala Político-Administrativa (SPA) del Tribunal Supremo de Justicia (TSJ). Cuando le corresponde conocer a la SPA, así como a los Juzgados Nacionales de la Región Capital, un abogado o la propia parte deben trasladarse hasta Caracas, ya que aún no existe en Venezuela otra forma de lograr el acceso a la justicia contencioso-administrativa si no es de manera presencial y en papel.

## Descripción de los procedimientos jurisdiccionales de primera instancia previstos en la LOJCA

El procedimiento de las pretensiones procesales administrativas de contenido patrimonial previsto en los artículos 56 al 64 de la LOJCA está compuesto por la interposición de la demanda y consignación de pruebas, admisión o despacho saneador y eventual inadmisión, la citación de la parte demandada; la notificación al procurador general de la República, en cuyo caso se suspenderá el proceso por noventa días para que el procurador general de la República decida si se hace parte; posteriormente, el juez podrá, de oficio o a petición de parte, convocar a la participación popular en la audiencia preliminar; la audiencia preliminar (en esta oportunidad puede darse el desistimiento tácito), la contestación de la demanda y presentación de prueba documental, la presentación de pruebas, el convenimiento sobre algún hecho u oposición a las pruebas, la admisión de las pruebas, la evacuación de las pruebas y por último se encuentran la audiencia conclusiva y la sentencia. Esto arroja como resultado que en este procedimiento existen, al menos, diez actos procesales escritos y dos actos procesales orales.

En cuanto al procedimiento breve, que se encuentra en los artículos 65 al 75 de la LOJCA, por el cual se tramitan reclamos por la omisión, demora o deficiente

1 La Ley Orgánica fue sancionada por la Asamblea Nacional el 15 de diciembre de 2009, y publicada en Gaceta Oficial No. 39.447 de 16 de junio de 2010, y luego reimpresa por "error material" en Gaceta Oficial No. 39.451 de 22 de junio de 2010.

2 Procedimiento de las pretensiones procesales administrativas de contenido patrimonial (Artículo 56. LOJCA), Procedimiento breve (Artículo 65. LOJCA: "Supuestos de aplicación" Reclamos por la omisión, demora o deficiente prestación de los servicios públicos; vías de hecho y abstención; que no tengan contenido patrimonial) y Procedimiento común a las pretensiones de nulidad, interpretación y controversia administrativa (Artículo 76. LOJCA: "Supuestos de aplicación". Este procedimiento regirá la tramitación de las demandas siguientes: 1. Nulidad de actos de efectos particulares y generales. 2. Interpretación de leyes. 3. Controversias administrativas).

3 El único procedimiento jurisdiccional que conoce es el de reclamo a los servicios públicos, previsto en el artículo 26 de la LOJCA.

4 Art 24 de la LOJCA.

5 Art 25 de la LOJCA.

prestación de los servicios públicos, vías de hecho y abstención, que no tengan contenido patrimonial, se requieren las actuaciones siguientes: interposición de la demanda, admisión de la pretensión, citación, notificación en casos de servicios públicos, notificación del procurador general de la República (si fuere el caso); admitida la demanda, el tribunal podrá de oficio o a instancia de parte, realizar las actuaciones que estime procedentes para constatar la situación denunciada y dictar medidas cautelares, la audiencia pública, y la sentencia. En este procedimiento existen alrededor de once actuaciones, las cuales están compuestas, aproximadamente, por diez actos procesales escritos y un acto procesal oral.

El procedimiento común a las pretensiones de nulidad, interpretación de ley y controversia administrativa, regulado en los artículos 76 al 86 de la LOJCA, tiene las siguientes actuaciones: interposición de la demanda, admisión de la pretensión o despacho saneador o subsanador, citaciones y notificaciones, requerimiento de expediente o antecedentes con la citación, cartel de emplazamiento, audiencia de juicio, admisión y evacuación de pruebas, informes y sentencia. Este procedimiento cuenta con menos actuaciones, pues tiene aproximadamente ocho, las cuales están compuestas por siete actos procesales escritos y un acto procesal oral.

Aunado a lo anterior es necesario recalcar que estas actuaciones no son las únicas que se encuentran en dicho procedimiento, ya que se pueden solicitar aclaratorias de sentencias, pedir u oponerse a medidas cautelares, además de recursos de apelación, amparos, y en general, se pueden abrir una serie de incidencias que van a multiplicar la cantidad de actos procesales, y esto se comprueba al revisar un expediente. Por tanto, se puede constatar en los procedimientos mencionados, la cantidad de veces, como mínimo, que tiene que acudir un particular ante la SPA, y está entre las doce, once y ocho veces, en el mismo orden como fueron expuestos los procedimientos, esto cuando la SPA conoce como primera y única instancia en cualquiera de los procedimientos antes señalados.

## Costos del acceso a la justicia contencioso-administrativa

Actuar en un proceso ante la Sala Político-Administrativa implica que las personas interesadas tengan que trasladarse a Caracas, específicamente al edificio del Tribunal Supremo de Justicia, al final de la avenida Baralt, esquina Dos Pilitas, municipio Libertador del Distrito Capital, para poder realizar las actuaciones procesales que atañen a sus intereses jurídicos, siempre y cuando sus pretensiones se relacionen con los aspectos relativos a su competencia, como lo establece el numeral 4 del artículo 226 de la Constitución, y desarrollado en el artículo 23 de la JOJCA.

Ahora bien, la ubicación del TSJ supone para las personas que no residen en Caracas, varios costos que deben cubrir, entre ellos se encuentran los gastos de transporte alimentación y pernocta, los honorarios profesionales y cualquier otro pago que se amerite. Para precisar los costos, se tomarán como muestras específicamente, cinco ciudades: Maracaibo, estado de Zulia; San Cristóbal, estado

de Táchira; Tucupita, estado de Delta Amacuro; Maturín, estado de Monagas y Puerto Ordaz, estado de Bolívar.

Primero para calcular los costos de transporte se deben considerar varios factores, como la distancia y el tipo de transporte o medio que se utilice, sea por vía terrestre, a través de vehículo privado o tren; o parcialmente por vía marítima, fluvial, y aérea, ya que el costo se calcula en función de estos y puede variar.

A fin de recaudar datos, se consultó el día 20 de abril de 2024, a través de la taquilla de atención al cliente, los precios de los pasajes de autobús con destinos a nivel nacional: Expresos Occidente y Expresos Guayana. Estos varían de acuerdo con la tasa del dólar de Estados Unidos de América, establecido por el Banco Central de Venezuela al momento de comprar el boleto, con las tasas de salida de la terminal incluidas, son los siguientes: Maracaibo, Zulia hasta Caracas por USD 28; San Cristóbal, Táchira hasta Caracas por USD 35; Tucupita, Delta Amacuro hasta Caracas por USD 35; Maturín, Monagas hasta Caracas por USD 20; y de Puerto Ordaz, Bolívar hasta Caracas por USD 31.

Otro medio de transporte que se podría utilizar sería el prestado por la empresa Ridery[6]. Los precios consultados a través de su aplicación, en esa misma fecha, fueron los siguientes: Maracaibo hasta Caracas por USD 246; San Cristóbal hasta Caracas por USD 342; Tucupita hasta Caracas por USD 255: Maturín hasta Caracas por USD 106; y Puerto Ordaz hasta Caracas por USD 295.

Por otro lado, los costos de los boletos del transporte aéreo consultados el mismo día, 20 de abril de 2024, a través de los números telefónicos publicados en los portales de internet de las aerolíneas Avior Airlines[7], pueden variar entre los USD 70 y 120 según la variación en el tiempo y del destino de 45 a 60 minutos. En la aerolínea Conviasa[8], los precios para vuelos desde Caracas hasta Maracaibo son de USD 120, desde Caracas con destino Maturín, USD 157, y desde Caracas hasta Puerto Ordaz, USD 120.

Por otro lado, el transporte terrestre particular implica costos de combustible que aumentarán por la cantidad de kilómetros que se recorra, en general, un vehículo de gama media, con una capacidad de combustible de 50 litros, tiene un costo de USD 25, esto quiere decir que esta cantidad de combustible será suficiente para recorrer aproximadamente 526 kilómetros antes de tener que llenar el tanque.

Para promediar los costos de combustible desde las cinco ciudades en estudio hasta Caracas, en un vehículo de gama media, los costos son los siguientes[9]: desde Maracaibo, la distancia es de 795,76 km, el costo en combustible sería de USD 38; desde San Cristóbal, la distancia es de 810 km, el costo sería de USD 39;

6 Tomado del portal de internet de Ridery: https://web.ridery.app/

7 Tomado del portal de internet de Avior Airlines: https://aviorair.com/vuelos

8 Tomado del portal de internet de Conviasa: https://aerolineasvenezolanas.net/conviasa/vuelos-nacionales-v0/

9 Para calcular los costos en combustible usaremos una regla de tres, fórmula matemática sencilla que nos aproximará a los costos por la compra del combustible; es decir, si un vehículo promedio con un tanque de gasolina de 50 litros recorre 526 kilómetros y su costo sería de USD 25, ya que el litro de gasolina a precio internacional está en USD 0,50$.

desde Tucupita, la distancia es de 719 km, el costo sería de USD 34; desde Maturín, la distancia es de 504 km, el costo sería de USD 24; desde Puerto Ordaz, la distancia es de 683 km, el costo sería de USD 33. Cabe recalcar que estas mismas cantidades de dinero se duplican al momento de realizar el retorno (Olguín, 2024).

A estos costos se suman los de alojamiento, porque las personas que deban acudir a Caracas, específicamente a la Sala Político-Administrativa, para consignar algún documento o revisar el expediente deberán estar en persona en las instalaciones del Tribunal en el horario de despacho comprendido desde las 8:30 a. m. a 3:30 p. m., siendo poco probable realizar los trámites en un solo día y retornar. Es por ello que lo más conveniente sería alojarse en un hotel cerca del TSJ.

En esa misma fecha se consultó las tarifas por noche de algunos hoteles y el costo es el siguiente: en el hotel El Arroyo, ubicado en la Av. Lecuna, USD 34; en el hotel Sil, ubicado en Sabana Grande, USD 20 hasta USD 30; y en el hotel Palas, ubicado en Quinta Crespo, USD 40 o, con desayuno, USD 50. Estos costos variarán dependiendo de la calidad del servicio y la ubicación del hotel, y se pueden promediar de USD 30 a USD 50 por noche.

A fin de determinar los costos de la alimentación me dirigí personalmente el día 20 de abril de 2024 a la Tasca Restaurant Royal, que se encuentra en Capitolio, y un desayuno completo tiene un costo de USD 8, un almuerzo varía de USD 8 a USD 14, igualmente una cena. En otro restaurante, Artesano Cafetería, los desayunos varían desde USD 3 hasta USD 6,90, las bebidas y cafés USD 1,30 a USD 2,30, y los almuerzos tienen un costo de USD 5,90 a USD 10, gastando entre las tres comidas alrededor de USD 30. Ahora, si la persona lo desea, puede comprar la comida por medio del portal de internet de Pedidos Ya, donde hay gran variedad de comidas y precios desde USD 7 y lo llevan a donde se encuentre.

Además de todos los costos anteriormente descritos, se podría sumar a ello, si el recurrente lo considera conveniente, cubrir los honorarios profesionales a abogados ubicados en Caracas en lugar de abogados de su localidad, para la consignación de escritos y revisión de expedientes, ya que estos abogados tienen mayor posibilidad de actuar ante el TSJ. Para el cobro de sus servicios tendrían que guiarse por el Reglamento Interno Nacional de Honorarios Mínimos[10], ya que su cumplimiento es de carácter obligatorio.

Después de haber obtenido varios presupuestos, es necesario indicar cuánto le cuesta a una persona acceder un día a la Sala Político-Administrativa y se tomará como muestra una de las ciudades en estudio: Maracaibo hasta Caracas, trasladándose en autobús, con la estadía en un hotel promedio y desayunando, almorzando y cenando, gastaría USD 98, gastos que pueden ser ahorrados por la implementación de plataformas que sustituyen los actos presenciales por actos procesales telemáticos escritos u orales, según el caso (Amoni, 2022, p. 452).

En el libro *Justicia digital en Iberoamérica a raíz del COVID 19* (Amoni, 2022, p. 518) se explica cómo se han usado soluciones de justicia digital, y qué

10 Art. 3 del Reglamento de honorarios mínimos profesionales, y los siguientes artículos.

debe tenerse en cuenta para que la tecnología pueda ser considerada como una contribución para el sistema judicial venezolano, ya que se profirieron varias resoluciones al respecto en función de contrarrestar los cambios que se produjeron durante la pandemia del covid-19, sin contar que ya existe legislación que puede coadyuvar con su implementación como la Ley de Mensajes de Datos y Firmas Electrónicas[11] y la Ley de Infogobierno[12].

Sobre el acceso a la justicia, Adriana Pereira Campos considera que la «Ley Orgánica de la Jurisdicción Contencioso Administrativa de 2010 diseñó una estructura de tribunales que aleja la justicia de los ciudadanos» (Pereira y Cornielles, 2017, p. 77). Entre los factores que afectan el acceso a la justicia está la pobreza, por esta razón, al hacer un estimado de los costos a los que se ve sometida una persona que vive en el interior del país para trasladarse a Caracas, a realizar las actuaciones del procedimiento de las pretensiones procesales administrativas de contenido patrimonial, se estima que como mínimo tiene que acudir ante la SPA, diez veces solo para realizar actuaciones por escrito, y dos veces para las audiencias que forman parte de las actuaciones orales, y como si fuera poco a esta cantidad de veces que la persona tiene que asistir ante la SPA, se le suman las consultas del expediente, la solicitud de copias e incidencias como aclaratorias de sentencia y, la solicitud de medidas cautelares, entre otras. Todo esto incrementa los costos, y se puede explicar brevemente cuando un abogado, y la propia parte, que se encuentre en Maracaibo tenga que trasladarse hasta Caracas, para acudir ante la SPA; si lo hace en autobús, con la estadía en un hotel promedio desayunando, almorzando y cenando gastaría USD 98 por día, al multiplicar esta cifra por la cantidad de actuaciones en el procedimiento pudiera costar USD 784 aproximadamente, solo en trasladarse hasta Caracas, sin considerar el retorno y los honorarios profesionales.

Esto quiere decir que el acceso a la Sala Política Administrativa resulta muy oneroso y con costos que pueden ser fácilmente evitados con la implementación de herramientas inherentes a las TIC, las cuales a partir de la pandemia por covid-19 se han desarrollado ampliamente en todo el mundo, lo cual no solo trae beneficios para el usuario sino también dinamiza y moderniza los procedimientos jurisdicciones llevados por la SPA como un órgano de competencia nacional que tiene una sede centralizada dentro del Tribunal Supremo de Justicia.

## Conclusiones

Se ha demostrado que la Sala Político-Administrativa, cuando conoce como primera y única instancia, requiere que los trámites que se realicen ante ella se hagan personalmente, y que el particular no solo debe cumplir con los requerimientos establecidos en la ley, sino también contar con la capacidad económica para asumir todos los costos que esto implica, lo cual también atenta indirectamente contra la gratuidad de la justicia consagrada en la Constitución de 1999,

11 Decreto n.º 1204 con rango y fuerza de ley sobre mensaje de datos y firmas electrónicas, publicado en Gaceta Oficial n.º 37.148, de fecha 28 de febrero de 2001.

12 Ley de Infogobierno, publicada en Gaceta Oficial n.º 40.274, de fecha 17 de agosto de 2013.

ya que no solamente los costos van por los aranceles judiciales, sino por lo complejo de tramitar un procedimiento ante dicha sala, teniendo su domicilio fuera de Caracas.

Por ello resulta necesario la digitalización de la justicia venezolana, ya que de esta manera los costos serían menores, y las personas realizarían todos los trámites desde un lugar con acceso a internet, o desde su teléfono celular, evitándose el traslado hasta Caracas para lograr la tutela de sus derechos, en consecuencia, es indispensable para la materialización de la tutela judicial efectiva en nuestra actual época tecnológica, la implementación de las TIC, tal como sucedió con los avances alcanzados durante la pandemia por covid-19, siendo mucho más económico y accesible para todos los abogados o partes que no se encuentran domiciliados en Caracas.

## Referencias bibliográficas

Amoni, G. (2022). Justicia Digital en Iberoamérica: a partir del COVID-19. En G. Amoni (Coord.), *Justicia Digital Coronavírica en Venezuela*.

Olguín, N. (2024). Calculadoras de gasto de gasolina: la solución para ahorrar combustible en segundos. *El Motor*. https://motor.elpais.com/conducir/aplicaciones-y-calculadoras-de-gasto-de-combustible/

Pereira, A., Cornielles, J. A. (2017). Estructura orgánica del contencioso administrativo en Venezuela (1976-2010). *Revista jurídica UNICURITIVA*, *4*(49).

Fundación
de Cultura
Universitaria

25 de Mayo 553 - Tel. 2916 1152
CP 11.000 Montevideo - Uruguay
libreria@fcu.edu.uy

**www.fcu.edu.uy**