ESTRATEGIA DE INTELIGENCIA ARTIFICIAL EN URUGUAY

Transparencia algorítmica, acceso a la información pública y protección de datos personales

BÁRBARA MURACCIOLE[1]

Revista de la Escuela del Cuerpo de Abogados y Abogadas del Estado | Mayo 2023 | Año 7 Nº 9 | Buenos Aires, Argentina (ISSN 2796-8642) | pp. 281-295

Resumen: La Organización para la Cooperación y el Desarrollo Económicos (OCDE) monitorea los avances de la Inteligencia Artificial a nivel mundial a través de su Observatorio de Políticas sobre Inteligencia Artificial (IA). En el marco de sus estudios sobre gobernanza pública, ha elaborado junto con la Banco de Desarrollo de América Latina (CAF) el informe denominado "Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe", en el cual destaca a Uruguay como el único país de América Latina y el Caribe que posee una estrategia específica de reestructuración del sector público por medio de la IA (OECD/CAF, 2022). Este artículo pretende analizar la estrategia de inteligencia artificial uruguaya en el contexto normativo nacional, particularmente de la Ley Nº 18.381, de 17 de octubre de 2008 sobre acceso a la información pública y Nº 18.331, de 11 de agosto de 2008 de protección de datos personales. Ello, a efectos de determinar si es

1 Doctora en Derecho y Ciencias Sociales, Facultad de Derecho, Universidad de la República Oriental del Uruguay. Máster en Protección de Datos, Universidad UNED, España. Profesora del Máster sobre el Reglamento Europeo de Protección de Datos para Iberoamérica, Universidad UNED, España. Docente de Derecho Informático e Informática Jurídica I y II, Facultad de Derecho, Universidad de la República Oriental del Uruguay. Integrante de la Asesoría Jurídica de la Presidencia de la República Oriental del Uruguay. Consultor privado en temas de su especialidad.

posible su aplicación práctica en términos de transparencia activa y pasiva y del derecho de las personas de conocer los procesos utilizados en la toma de decisión de los organismos públicos, en tanto la estrategia plantea el doble rol del Estado que debe, a la vez, rendir cuentas y controlar los procesos algorítmicos, al menos públicos.

Palabras clave: Inteligencia Artificial, Uruguay, estrategia, transparencia.

Abstract: The Organization for Economic Cooperation and Development (OECD) monitors the advances of Artificial Intelligence worldwide through its Artificial Intelligence (AI) Policy Observatory. Within the framework of his studies on public governance, he has prepared, together with the Development Bank of Latin America (CAF), the report entitled "Strategic and responsible use of artificial intelligence in the public sector of Latin America and the Caribbean", in the which highlights Uruguay as the only country in Latin America and the Caribbean that has a specific strategy for restructuring the public sector through AI (OECD/CAF, 2022). This article intends to analyze the Uruguayan artificial intelligence strategy in the national regulatory context, particularly Law No. 18.381, of October 17, 2008, on access to public information and No.18.331, of August 11, 2008, on the protection of personal data. This, in order to determine if its practical application is possible in terms of active and passive transparency and the right of people to know the processes used in decision-making by public bodies, while the strategy proposes the double role of the State which must, at the same time, be accountable and control algorithmic processes, at least public ones.

Keywords: Artificial Intelligence, Uruguay, strategy, transparency.

I. ESTRATEGIA DE INTELIGENCIA ARTIFICIAL DEL ESTADO URUGUAYO

En el año 2018, los países integrantes del Digital 9 (D9) conocidos como los países más avanzados digitalmente, entre los que se encuentra Uruguay, pautaron una serie de objetivos generales sobre la aplicación y el uso de la IA por parte de los gobiernos que integraban (AGESIC, 2018). A partir del 2019 conformaron un grupo de trabajo para compartir y generar conocimientos sobre la temática, tales como, marcos de referencia para un uso responsable y análisis de impacto ante el desarrollo de algoritmos y modelos.

Concomitantemente, a nivel nacional, se trabajó en la elaboración

de una estrategia que permitiera al Estado uruguayo utilizar la IA como herramienta para la transformación digital y que promoviera su uso responsable en la Administración Pública. Así nace la Estrategia de Inteligencia Artificial para el Gobierno Digital (la Estrategia) conjugando miradas éticas, normativas, técnicas y sociales, que se traducen en cuatro dimensiones de abordaje (AGESIC, 2019).

Según el documento, la **dimensión ética** reposa sobre "... *la transparencia en el accionar de la Administración Pública. Esta transparencia no sólo implica un conocimiento completo de la información gestionada, sino también de las estrategias aplicadas, sus fines y contenidos. Al mismo tiempo, mediante la introducción de reglas de transparencia se mitigarán las posibilidades de sesgos y discriminaciones no deseadas*".

Por su parte, la **dimensión legal** importa el respeto del marco jurídico preexistente, especialmente de los Derechos Humanos consagrados en instrumentos internacionales "*lo que asegura el equilibrio entre los derechos de las personas y la limitación del ámbito de actuación estatal*". La dimensión técnica refiere al cumplimiento de los marcos técnicos y normativos que garanticen la solvencia y solidez de los sistemas de IA y la **social se expresa en** generar soluciones orientadas a las personas.

Asimismo, la Estrategia enuncia los siguientes principios rectores: a) la finalidad, potenciadora de las capacidades humanas para mejorar la calidad de vida de las personas, facilitar procesos y aportar valor agregado a la actividad humana, b) el interés general, garante de la inclusión y la equidad, c) el respeto de los Derechos Humanos, las libertades individuales y la diversidad, d) la transparencia de las soluciones utilizadas en el ámbito público, e) la responsabilidad de personas físicas o jurídicas determinadas, f) la ética, g) el valor agregado y h) la privacidad por diseño y por defecto.

II. TRANSPARENCIA

A los efectos de presente trabajo nos centraremos en el reiterado concepto de transparencia de la actividad administrativa y los procesos algorítmicos, utilizado como fundamento de la dimensión ética y como principio rector de la Estrategia.

En Uruguay, la transparencia en el obrar de la Administración se encuentra plasmada en la Ley N° 18.381, de 17 de octubre de 2008, cuyo artículo 1° establece: *"La presente ley tiene por objeto promo-*

ver la transparencia de la función administrativa de todo organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública."

La transparencia refiere a un concepto más amplio que el de la publicidad, en tanto no sólo implica publicar, sino visualizar el actuar y la gestión de la Administración. Su faceta activa se relaciona con los datos publicados por los organismos obligados, mientras que la pasiva corresponde a las respuestas brindadas por la Administración ante solicitudes de información que le son formuladas.

Estamos ante *"uno de los valores más preciados en la actualidad. Muchos factores están convergiendo para que esto ocurra. Uno de ellos, indudablemente, es el debilitamiento que se ha producido en el mundo occidental de los autoritarismos, los que, por definición, están reñidos con la libre movilidad de la información. La revalorización consiguiente de la democracia y en especial de la libertad, ha traído consigo la rebeldía con el hecho de que sean otros los que decidan qué cosas debe conocer la ciudadanía. América Latina no ha sido ajena a este movimiento. Es más, buena parte de las leyes que en la región expresamente garantizan el libre acceso a la información pública han sido promovidas por organizaciones de la sociedad civil, en particular, de medios de comunicación que reivindican la circulación de la información como vehículo de libertad"* (Grau, 2006).

Al respecto, recientemente, el Tribunal de Apelaciones en lo Civil de 7° Turno, parafraseando a la Suprema Corte de Justicia Uruguaya, sostuvo: *"tanto el derecho a la información como la libertad de prensa son derechos tan trascendentes que pueden ser ubicados en un plano superior al de otros derechos civiles, pues de ello depende la estructura de las relaciones entre el poder y la libertad"* (Sentencia N° 20/2023, 2023).

De lo dicho resulta, que la Estrategia no aporta valor en términos sustantivos, puesto que enuncia un actuar ya reglado para la Administración nacional, limitándose a reafirmar un concepto previamente recogido por el legislador patrio y ampliamente recibido por nuestra jurisprudencia.

Relacionado con los algoritmos, la Estrategia establece que las soluciones de IA utilizadas en el ámbito público deben ser transparentes, lo que se logra: a) poniendo a disposición los algoritmos y datos utilizados para el entrenamiento de la solución y su puesta en práctica, así como las pruebas y validaciones realizadas, y b) visibi-

lizando explícitamente, a través de mecanismos de transparencia activa, todos aquellos procesos que utilicen IA, ya sea en la generación de servicios públicos o en el apoyo a la toma de decisiones.

Significa que la Estrategia le impone al Estado la obligación de publicar (transparencia activa) los datos, procesos y validaciones aplicados por las soluciones de IA que utilice en el ejercicio de sus funciones.

¿Es esto viable? ¿Pueden los organismos públicos en Uruguay comunicar datos o publicar información relativa a las licencias de software que utilizan?

Sí es posible, siempre que se trate de datos personales que no estén sujetos al previo consentimiento informado de sus titulares, que su publicación no vulnere normas de propiedad intelectual ni cláusulas contractuales de confidencialidad, porque en dichos supuestos, estaríamos ante excepciones al derecho de acceso a la información pública y la Administración no sólo no podría entregar dichos datos, sino que estaría impedida de hacerlo.

En efecto, en Uruguay toda persona física o jurídica puede acceder a la información pública en poder de los organismos públicos, sean estatales o no (artículos 3° y 13 de la Ley N° 18.381). Por información pública se considera la que emane o esté en posesión de dichas entidades, salvo la exceptuada por ser secreta, reservada o confidencial (artículos 2°, 4° y 8° de la citada Ley).

Siguiendo a Carlos Guariglia: *"Sabemos, que los derechos humanos no sólo tienen un carácter universal, son indivisibles, complementarios, inalienables o inviolables, sino que por imperio de la alteridad humana, ellos obedecen a límites generales, normales, ordinarios, como también existen circunstancias en que es menester el reconocimiento de límites excepcionales como extraordinarios ... los límites externos son los que impiden el conflicto entre los derechos fundamentales, tendiendo a armonizar el derecho de que se trate con otros derechos y con otros bienes constitucionales"* (Guariglia, 2007).

La información secreta es aquélla definida por ley que no requiere un acto de la Administración para serlo, ya que representa la voluntad del legislador. Es el caso del secreto profesional, bancario, tributario, estadístico, entre otros.

Por su parte, la información reservada se relaciona con los cometidos esenciales del Estado, tales como el orden y seguridad internos, la defensa nacional, las relaciones exteriores y la actividad financiera, económica y científica del Estado, cuya revelación podría afectar

la integridad y los derechos de las personas, las libertades, el orden y la paz pública, así como la actuación del Estado como sujeto de Derecho Internacional. La Administración puede reservarla mediante un acto de clasificación, siempre que *"demuestre la existencia de elementos objetivos que permitan determinar que la divulgación de la misma genera un riesgo claro, probable y específico de daño al interés público protegido"* (artículo 9° de la Ley N° 18.381).

La confidencialidad, refiere a la información de las personas físicas y jurídicas en poder de la Administración. Esta excepción protege directamente el derecho a la vida privada, los datos personales, el patrimonio de las personas, así como los datos comerciales de éstas que pudieren ser útiles para su competencia, motivo por el cual puede ser clasificada (artículo 10 de la Ley N° 18.381).

Al decir de la Unidad de Acceso a la Información Pública -organismo garante del derecho de acceso en nuestro país-, resguardando este tipo de información: "*se busca proteger una serie de conocimientos técnicos que poseen valor comercial, desarrollados por sus empresas y que pueden ser útiles para sus competidores. Esta serie de conocimientos técnicos deben mantenerse fuera del alcance de terceros, pero sobre todo fuera del alcance de los competidores de esas empresas, como forma de evitar la competencia desleal"* (Unidad de Acceso a la Información Pública).

Dentro de este marco tasado de excepciones, encontramos, sin duda, información relativa a los desarrollos de software que utilizan IA y que los organismos públicos contratan, los cuales, en su mayoría, se encuentran sujetos a licencias de uso que determinan restricciones en la revelación de información. Esto, debido a que las empresas y personas físicas legítimamente amparadas en normas de propiedad intelectual y en cláusulas de confidencialidad, resguardan sus productos (algoritmos) y su *know how* de otros competidores.

Recordemos que el inciso final de la Ley N° 9.739, de 17 de diciembre de 1937 sobre Derechos de Autor, en la redacción dada por el artículo 3° de la Ley N° 17.616, de 10 de enero de 2003 protege: *"Programas de ordenador, sean programas fuente o programas objeto; 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. Esta 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. La expresión*

de ideas, informaciones y algoritmos, en tanto fuere formulada en secuencias originales ordenadas en forma apropiada para ser usada por un dispositivo de procesamiento de información o de control automático, se protege en igual forma. Y, en fin, toda producción del dominio de la inteligencia".

También son pasibles de ampararse en dichas excepciones los datos personales sujetos al consentimiento, los que no deben comunicarse (publicarse, dar acceso) sin autorización previa, expresa e informada de sus titulares (artículos 9° y 17 de la Ley N° 18.331, de 11 de agosto de 2008), o se afectaría el derecho a la protección de datos personales de los involucrados.

Vemos entonces, al contrastar la Estrategia con el marco normativo imperante en materia de transparencia, acceso a la información pública y protección de datos personales, que sus recomendaciones coliden con disposiciones normativas expresas y la tornan inaplicable para los organismos públicos que son los destinatarios. Ello, debido a que la transparencia solicitada no reposa en información pública y, por tanto, la Administración no sólo no estaría obligada a revelarla sino que estaría impedida de hacerlo.

Paradójico y sin salida se presenta el camino de la transparencia algorítmica elegido por la Estrategia de Inteligencia Artificial del Estado uruguayo.

¿Cómo proteger a las personas si las normas vigentes no permiten transparentar la actividad algorítmica de la Administración y acceder a la información detrás del funcionamiento de la IA utilizada por el Estado? Quizás la salida se encuentre en un cambio de enfoque ¿será la transparencia algorítmica la solución, la única alternativa?

III. GUBERNAMENTALIDAD ALGORÍTMICA

La opacidad de los procesos algorítmicos sumada a su omnipresencia, han desencadenado opiniones críticas que sugieren que estamos gobernados por los algoritmos en tanto aceptamos la utilización de sistemas que no sabemos cómo funcionan y, por ende, no somos capaces de controlar. Así, es usual leer o escuchar que estamos ante un imperio o gobierno de los algoritmos, o ante una algoritmocracia.

Personalmente, encuentro interesante el abordaje realizado por la filósofa del Derecho Antoinette Rouvroy quién, partiendo del concepto de gubernamentalidad de Michel Foucault –que refiere a la idea de una articulación entre formas de saber y relaciones de

poder que establece un gobierno sobre los sujetos–, explica este fenómeno como un nuevo modo de ejercicio del poder que ya no reside en las normas impuestas por el Estado, sino en el análisis de las innumerables trazas digitales sobre las actitudes y comportamientos de las personas, al que denomina: gubernamentalidad algorítmica (Muracciole, 2018).

Su mirada, no sólo ha sido crítica ante los riesgos de estos desarrollos, sino también ante las soluciones planteadas. Así, desde los inicios de las discusiones, Rouvroy discrepó con la elogiada transparencia algorítmica por considerar inviable explicar y comprender el procesamiento de información que estos desarrollos son capaces de lograr en microsegundos.

En el año 2018 no coincidía en este punto con Rouvroy. Al igual que la doctrina técnica y jurídica mayoritaria, consideraba que la revelación y puesta a disposición del funcionamiento de los algoritmos (incluidos los de IA) era la mejor forma de proteger los derechos y libertades. Me parecía que democratizar la información generaría un control social y una sensibilización sobre los impactos, empoderando a las personas usuarias.

Hoy, comparto la discrepancia y la considero más vigente que nunca. La realidad ha demostrado que las exigencias de transparencia en materia algorítmica no prosperaron. Por un lado, porque chocan con normas de propiedad intelectual, por otro, porque aun en conocimiento de toda la información relativa a un algoritmo basado en el uso de IA, los usuarios no serían capaces de comprender el funcionamiento y tampoco de medir las consecuencias al momento de prestar su consentimiento o incluso de adquirir un desarrollo que utilice IA.

Entonces ¿de qué sirve más información que no se puede comprender? ¿Simplemente con informar al usuario se evitan los riesgos que el uso del desarrollo de IA le puede acarrear? A la luz de los avances actuales, la prudencia señala que no. No basta con informar, mucho o poco, para evitar lesiones y vulneración de derechos (discriminación, estigmatización). Esto no implica que no se deba informar, esto significa que con sólo hacerlo no basta, que la realidad le muestra al jurista que otras acciones de protección son necesarias. En este sentido, la legislación internacional avanza en modelos preventivos y no reactivos.

Sin perjuicio, el escenario jurídico nacional continúa transitando el camino de solicitar más información como forma de tutela.

Recientemente fue modificada la normativa de protección de datos personales a fin de disponer que, cuando se recaben datos para utilizarlos en tratamientos automatizados, se deberán informar: *"los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizado"* (literal G) del artículo 13 de la Ley N° 18.331, de 11 de agosto de 2008, en la redacción dada por el artículo 62 de la Ley N° 20.075, de 20 de octubre de 2022).

El artículo 16 de la Ley N° 18.331, que regula el derecho de las personas a no verse sometidas a una decisión con efectos jurídicos que las afecte de manera significativa, ya preveía que se pudiera obtener dicha información. El cambio legislativo resulta en que ya no será necesario pedirlo, sino que deberá ser previamente informado/publicado por el responsable del tratamiento de los datos. Valen en esta instancia los comentarios vertidos en torno al posible amparo de tal información en normas de propiedad intelectual.

Una solución similar al citado artículo 16 se encuentra en el artículo 22 del Reglamento General de Protección de Datos 2016/679 de la Unión Europea (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo , 2016).

No obstante, según mencionara, la Unión progresa y complementa su normativa de protección de datos personales. Así, la Propuesta del Parlamento Europeo y del Consejo de un Reglamento en materia de Inteligencia Artificial *"sigue un enfoque basado en los riesgos y únicamente impone cargas normativas cuando es probable que un sistema de IA entrañe altos riesgos para los derechos fundamentales y la seguridad. A los demás sistemas de IA que no son de alto riesgo tan solo se les imponen obligaciones muy limitadas en materia de transparencia; por ejemplo, en lo que se refiere a la presentación de información para comunicar el uso de un sistema de IA cuando este interactúe con humanos"* (punto 2.3 de la exposición de motivos). Recordemos que este proyecto fue publicado en abril de 2021 por el Parlamento Europeo y el Consejo de la Unión Europea (Propuesta de Reglamento IA, 2021).

Según dicha propuesta normativa, los sistemas de IA se clasifican en: riesgo mínimo (mayoría de IA y serán de uso libre, por ejemplo: filtros de spam), riesgo limitado (los ciudadanos deben ser conscientes que interactúan con IA, por ejemplo: chatbot), alto riesgo (tendrán obligaciones estrictas, como supervisión humana y el uso de datos de alta calidad para evitar la discriminación, por ejemplo: sistemas para otorgar créditos) y riesgo inaceptable (estos sistemas

estarán prohibidos, por ejemplo: puntuación social de los gobiernos).

IV. NUEVOS CAMINOS Y PARÁMETROS

A nivel nacional, la Academia también señala la necesidad de explorar nuevos rumbos. Con fecha 10 de marzo de 2023, en el marco del Encuentro Latinoamericano de Inteligencia Artificial (Khipu) en la Facultad de Ingeniería de la Universidad de la República, se produjo la "Declaración de Montevideo sobre Inteligencia Artificial y su impacto en América Latina" (Declaración de Montevideo, 2023).

Este documento introduce nuevos parámetros a considerar en la investigación y desarrollo de las tecnologías en general y los sistemas de Inteligencia Artificial en particular. Coincidentemente con lo que venimos analizando, la transparencia algorítmica no se menciona, en su lugar se exhorta a:

- respetar y representar las diferencias culturales, geográficas, económicas, ideológicas y religiosas, entre otras, y no reforzar estereotipos o profundizar la desigualdad,
- no dañar a las personas y minimizar el impacto ambiental,
- suspender tecnologías con riesgos inaceptables, atender la problemática del empleo, atender la diversidad cultural desde el diseño reposicionando el acervo cultural latinoamericano,
- integrar las particularidades latinoamericanas, valorando su participación en investigación y desarrollo, y no sólo como meros productores de datos en bruto o anotaciones manuales con bajo valor agregado, y
- fortalecer la soberanía de los países latinoamericanos con respecto a las cuestiones estratégicas y regulatorias de la IA.

La declaración finaliza con una propuesta para "desarrollar criterios y estándares que permitan calificar estas tecnologías según sus riesgos, para avanzar en políticas públicas que protejan el bien común sin obturar los beneficios del desarrollo tecnológico".

Luego de la propuesta, la Declaración menciona que desde "la concepción de una solución tecnológica basada en IA y no después de creada, debemos preguntar cuál es el valor social que aporta y los riesgos que conlleva, con una mirada informada de la idiosincrasia latinoamericana. También es necesario analizar y comunicar honestamente sus limitaciones, sin exagerar sus capacidades ni hacer promesas inconducentes".

Indudablemente, ya no basta con hablar de privacidad o seguridad

desde el diseño o por defecto, pretendiendo que las normas sobre protección de datos personales sean la respuesta a todos los problemas del mundo digital, la mirada debe ser más amplia e integradora, debe ser social.

El documento culmina expresando: "No hay valor social en tecnologías que simplifican tareas a unas pocas personas generando alto riesgo para la dignidad de muchas otras, limitando sus oportunidades de desarrollo, su acceso a recursos y sus derechos".

Al igual que el Parlamento Europeo, la Declaración de Montevideo parte del riesgo intrínseco en el uso de IA, el cual nuestra legislación ya no debería ignorar, sino determinar y reglar.

Si el riesgo aparece como una variable evidente en el uso de la Inteligencia Artificial ¿qué respuesta jurídica proactiva y no reactiva podríamos utilizar para contenerlo? La doctrina regional promueve la aplicación del principio precautorio a tales efectos.

V. PRINCIPIO PRECAUTORIO

Según la Real Academia Española, riesgo proviene *del ant. riesco ´risco´, por el peligro que suponen*, se trata de una *contingencia o proximidad de daño*.

Siguiendo las enseñanzas del Profesor Marcus Filgueiras, estamos ante un principio que se originó en el Derecho alemán en la década del 70, cuando existía una preocupación por la evaluación previa de las consecuencias de las intervenciones sobre el medio ambiente, cobrando importancia debido al deseo desmesurado del hombre de hacer uso de la tecnociencia para dominar la naturaleza (Filgueiras, 2022).

De histórica aplicación en la protección del medio ambiente, su definición pacíficamente aceptada es la proporcionada en la Declaración de Río sobre el Medio Ambiente y el Desarrollo: *"Principio 15: Con el fin de proteger el medioambiente, los Estados deberán aplicar ampliamente el criterio de precaución conforme a sus capacidades. Cuando haya peligro de daño grave o irreversible, la falta de certeza científica absoluta no deberá utilizarse como razón para postergar la adopción de medidas eficaces en función de los costos para impedir la degradación del medio ambiente"* (Declaración de Río sobre el Medio Ambiente y el Desarrollo, 1992).

En palabras del Tribunal de lo Contencioso Administrativo, su "*contenido implica inhibir tanto al Estado como a los particulares de*

desarrollar conductas cuya potencialidad dañosa para el medioambiente, no ha sido científicamente descartada. Tal temperamento encuentra respaldo en los arts. 3, 4 y 6, lit. B), de la Ley 17.283, art. 1 Ley 16.466, art. 11.2 Protocolo a la Convención Americana sobre Derechos Humanos "Protocolo de San Salvador" aprobado por Ley 16.519, y, se compadece con la línea trazada por el constituyente en el art. 47 de la Constitución de la República" (Tribunal de lo Contencioso Administrativo, 2021)

Citando a Ricardo Lorenzetti, la Corporación señala*: "El principio precautorio reconoce que demorar la acción hasta que exista una completa evidencia de la amenaza, a menudo significa que será muy costoso o imposible evitarla. También se produce un traslado del riesgo de la demora en actuar, lo que tradicionalmente fue un elemento neutro que generaba costos para el ambiente. Cuando surge una duda en la regulación, normalmente se pospone para buscar mayores seguridades o bien hasta que surja algún elemento nuevo que permita apreciar los hechos con mayor claridad. El* principio precautorio *introduce una excepción en esta materia al comparar los costos de la demora con los de la conducta proactiva, y postula que siempre es menos grave actuar que demorar en hacerlo. Avanzando sobre las duda y sin demoras, importa que los riesgos de la actuación precipitada los soporta el peticionante"* (Lorenzetti, 2008).

En este contexto, Filgueiras entiende: "*que la utilización de tecnología que pueda afectar la vida humana se ajusta al complejo fáctico que debe alcanzar el principio precautorio*" por lo que sería trasladable a la utilización de la IA (Filgueiras, 2022). Posición que comparto.

Pero no todas las voces resultan coincidentes. Esta solución despierta críticas que señalan que: "todos los aspectos del Principio Precautorio son discutibles: el grado de certeza científica necesario para proscribir una actividad riesgosa; si la autoridad debe limitarse a la evidencia científica disponible o puede seguir las máximas de la experiencia y el sentido común; si el Principio Precautorio opera más allá de los riesgos tecnológicos que amenazan la vida, la salud humana y el entorno; si la gravedad e irreparabilidad del daño son requisitos copulativos o alternativos; si las medidas de precaución deben suprimir o solo reducir el riesgo a un nivel razonable; si es un principio programático, preceptivo, político, interpretativo o un mero argumento jurídico" (Banfi, 2019).

VI. REFLEXIONES

La Estrategia de Inteligencia Artificial en Uruguay le impone al Estado exigencias que no podrá cumplir. La transparencia algorítmica solicitada reposa, en su mayoría, en información exceptuada del acceso público que impide a la Administración su revelación. De todas formas, la fallida práctica de la transparencia algorítmica ha demostrado que más información no resulta en mayor protección de los derechos y libertades frente a los desarrollos de la Inteligencia Artificial.

La realidad le impone al jurista transitar otros caminos y aportar una mirada amplia e integradora, desde una lógica social. No bastan las normas en materia de privacidad y protección de datos personales para abarcar los problemas que presenta el mundo digital. El riesgo aparece como una variable intrínseca y evidente en el uso de la Inteligencia Artificial que no es posible evitar ni valorar a *posteriori.* Es necesario trabajar en respuestas legislativas proactivas para contenerlo, cuando así sea necesario.

El principio precautorio se abre camino en la doctrina regional y nos propone inhibir conductas cuya potencialidad dañosa no ha sido científicamente descartada. Legislar en supuestos de inhibición o prohibición de sistemas de Inteligencia Artificial con riesgos inaceptables, es una posibilidad que debe ser explorada a nivel nacional y regional.

"*Aun cuando no lo parezca, dice Sadin, la inteligencia artificial termina por limitar la capacidad de juicio, reemplazándola. Pero la cuestión, está, cabe decir, en si esto es en sí un antivalor. Cabe pensar que la "ayuda" es bienvenida; mas, el "control" y reemplazo de lo humano, así como la determinación de la vida por tales controles, no lo parece. Tampoco se trata de la idea según la cual lo digital terminará por "destruir" lo humano; más bien el punto es que, sin destruir nada, sí habría el peligro de mayor sometimiento a las decisiones tomadas por programas, por algorítmicos procesos, más allá del juicio humano. Un nuevo derecho, pues, ya no divino sino digital*" (Ramírez, 2021).

REFERENCIAS BIBLIOGRÁFICAS

AGESIC. (2018). *Uruguay asumió la presidencia del D9*. Obtenido de https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-asumio-presidencia-del-digital-9

AGESIC. (2019). *Estrategia de Inteligencia Artificial.* Obtenido de Estrategia de Inteligencia Artificial para el Gobierno Digital: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia%20IA%20-%20versi%C3%B3n%20espa%C3%B1ol.pdf

Banfi, C. (2019). Riesgos en la aplicación del principio precautorio en responsabilidad civil ambiental. *Revista Chilena de Derecho*.

Declaración de Montevideo. (10 de marzo de 2023). Obtenido de Declaración de Montevideo sobre Inteligencia Artificial y su impacto en América Latina: https://docs.google.com/document/d/1maoIc9BKnJbM_iv1QXvbU0DofgmmOQne3qjmQb0rFHM/edit

Declaración de Río sobre el Medio Ambiente y el Desarrollo. (junio de 1992). Obtenido de https://www.un.org/spanish/esa/sustdev/agenda21/riodeclaration.htm

Filgueiras, M. V. (2022). La Inteligencia Artificial en la Administración Pública Barsilera: la interpretación legal a la luz del principio precautorio y democrático. *Electronic Journal of Sadio*, págs. 70-86.

Grau, N. C. (2006). La transparencia en la gestión pública ¿Cómo construirle vialidad? *Revista Chilena de Administración Pública*, 22 a 44.

Guariglia, C. (2007). Límites, delimitación o restricción de los derechos fundamentales. En *El conflicto entre los Derechos Fundamentales* (pág. 191). Amalio Fernández.

Lorenzetti, R. (2008). *Teoría del Derecho Ambiental.* La Ley.

Muracciole, B. (2018). El derecho en tiempo de algoritmos. En C. Cobo, *Jóvenes, transformación digital y formas de inclusión en América Latina* (pág. 275 a 286). Montevideo: Penguin Random House.

OECD/CAF. (2022). *Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe, Estudios de la OCDE sobre Gobernanza Pública.* Paris: OECD Publishing.

Propuesta de Reglamento IA. (21 de abril de 2021). Obtenido de Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial del Parlamento Europeo y del Consejo: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

Ramírez, A. (2021). Éric Sadin. La inteligencia artificial o el desafío del siglo. Anatomía de un antihumanismo radical. *Revista de Filosofía, Universidad de Chile*.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo . (27 de abril de 2016). Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=ES

Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión. (2021). Unión Europea.

Sentencia N° 20/2023 (Tribunal de Apelaciones en lo Civil de 7° Turno 23 de febrero de 2023).

Tribunal de lo Contencioso Administrativo, 30/2021 (Tribunal de lo Contencioso Administrativo 9 de febrero de 2021).

Unidad de Acceso a la Información Pública. (s.f.). *Guía e instructivo práctico para clasificar información como reservada o confidencial.* Obtenido de https://www.gub.uy/unidad-acceso-informacion-publica/comunicacion/publicaciones/guia-instructivo-practico-para-clasificar-informacion-reservada