PROYECTO DE RESOLUCIÓN

La Honorable Cámara de Diputados de la Nación

RESUELVE:

Dirigirse al Poder Ejecutivo Nacional, en ejercicio de las facultades conferidas por los artículos 75 inciso 32 de la Constitución Nacional y 204 del Reglamento de la Honorable Cámara de Diputados de la Nación, para que, a través de los organismos que correspondan, informe acerca de los anuncios vinculados a la implementación, desarrollo o utilización de sistemas de inteligencia artificial, modelización predictiva, interoperabilidad masiva de datos y/o construcción de denominados "gemelos digitales" aplicados al diseño, simulación, evaluación o ejecución de políticas públicas, detallando especialmente:

1. Informe si el Poder Ejecutivo Nacional desarrolla, implementa, financia, evalúa o proyecta la utilización de sistemas de inteligencia artificial, modelización predictiva, analítica avanzada, simulación social o construcción de denominados "gemelos digitales" destinados al diseño, simulación, ejecución, evaluación o proyección de políticas públicas.

2. Indique cuál es la denominación oficial del programa, sistema, iniciativa, plataforma o proyecto involucrado, precisando organismo responsable, autoridades intervinientes, unidades ejecutoras y dependencias estatales participantes.

3. Informe si existe acto administrativo, resolución, decisión administrativa, convenio, acuerdo de cooperación, contratación, licitación o cualquier otro instrumento formal vinculado al desarrollo, implementación o utilización del sistema, remitiendo copia íntegra de toda la documentación correspondiente, incluidos anexos técnicos, dictámenes jurídicos, informes de impacto, estudios preliminares y documentación contractual.

4. Informe qué partidas presupuestarias financian el desarrollo o implementación del sistema, precisando si los fondos fueron previstos en la Ley de Presupuesto Nacional vigente o si se financian mediante reasignaciones presupuestarias, fondos fiduciarios, créditos internacionales u otros mecanismos extraordinarios.

5. Precise si intervienen organismos multilaterales de crédito, organismos internacionales, agencias extranjeras o entidades privadas en el financiamiento, asistencia técnica o desarrollo del sistema, indicando condiciones, cláusulas, compromisos asumidos y términos de cooperación celebrados.

6. Informe el costo total estimado o contractual del sistema, discriminando etapas de diseño, desarrollo, implementación, mantenimiento, almacenamiento de datos, infraestructura tecnológica y servicios asociados.

7. Informe qué organismos públicos nacionales participan o participarían del intercambio, procesamiento, interoperabilidad o cesión de datos vinculados al sistema.

8. Precise si existen acuerdos de intercambio de información con provincias, municipios, universidades, empresas privadas, organismos internacionales o entidades extranjeras.

9. Informe si el sistema contempla mecanismos de interoperabilidad automática entre bases de datos estatales, precisando alcance, finalidad y fundamento normativo habilitante.

10. Precise si se prevé el acceso, consulta, procesamiento o cruce de información proveniente de:

    a. Registro Nacional de las Personas (RENAPER);
    b. Administración Federal de Ingresos Públicos (AFIP/ARCA);
    c. Administración Nacional de la Seguridad Social (ANSES);
    d. Programa de Atención Médica Integral (PAMI);
    e. Sistema de Identificación Nacional Tributario y Social (SINTyS);
    f. Ministerio de Salud;
    g. Ministerio de Educación;
    h. padrón electoral nacional;
    i. registros biométricos;
    j. historias clínicas;
    k. bases de datos tributarias, patrimoniales o previsionales;
    l. información georreferenciada o de geolocalización;
    m. información proveniente de redes sociales;
    n. antecedentes administrativos o judiciales;
    o. cualquier otra base de datos sensible en los términos de la Ley N° 25.326.

11. Precise el fundamento legal que habilitaría el acceso, procesamiento, interoperabilidad o utilización de cada una de las bases de datos involucradas.

12. Informe qué tipos de datos personales serían utilizados por el sistema, indicando si se prevé el tratamiento de datos identificatorios, biométricos, sanitarios, educativos, financieros, tributarios, laborales, previsionales, conductuales o sensibles.

13. Indique si los datos serán anonimizados, pseudoanonimizados o individualizados, precisando mecanismos técnicos de anonimización, cifrado, seguridad informática y resguardo de información que serían aplicados.

14. Informe cuáles serán los plazos de almacenamiento, conservación y eliminación de los datos utilizados, así como los protocolos previstos para su destrucción segura.

15. Informe si los datos del sistema serán almacenados en infraestructura estatal ubicada en territorio nacional o en servicios de nube provistos por empresas privadas nacionales o

extranjeras, incluyendo Amazon Web Services (AWS), Google Cloud, Microsoft Azure u otras plataformas similares.

16. Precise si existe riesgo de almacenamiento, procesamiento o transferencia internacional de datos personales de ciudadanos argentinos, indicando qué medidas se adoptarían para prevenir cesiones indebidas de información o pérdida de soberanía tecnológica.

17. Informe qué jurisdicción legal resultaría aplicable en caso de conflicto con proveedores extranjeros y si los contratos suscriptos contienen cláusulas de sometimiento a tribunales, arbitrajes o legislación extranjera.

18. Informe si el Estado Nacional conserva la titularidad, propiedad, control y acceso irrestricto respecto del código fuente, modelos algorítmicos, bases de datos y sistemas desarrollados, o si existen licencias, restricciones contractuales, acuerdos de confidencialidad o limitaciones técnicas que condicionen dicho acceso.

19. Precise si el Estado Nacional podrá reemplazar proveedores tecnológicos sin perder acceso a los sistemas, modelos entrenados, bases de datos o información procesada.

20. Informe si existe protocolo de discontinuación, desactivación o reversibilidad del sistema que garantice eliminación segura de datos, restitución de información y cese verificable de procesamiento automatizado.

21. Precise qué ocurrirá con los datos personales almacenados o procesados en caso de rescisión, vencimiento o finalización de contratos celebrados con proveedores privados.

22. Informe si el sistema prevé mecanismos de perfilamiento automatizado, clasificación poblacional, análisis conductual, segmentación social o generación de inferencias respecto de personas, grupos sociales, territorios o comunidades específicas.

23. Precise si el sistema podrá producir evaluaciones de riesgo, predicciones sociales, segmentaciones territoriales, proyecciones de comportamiento colectivo o recomendaciones automatizadas para orientar decisiones estatales.

24. Informe si se prevé la utilización de herramientas de inteligencia artificial generativa, machine learning, deep learning, sistemas predictivos, modelos de scoring o cualquier otro mecanismo automatizado de análisis masivo de información.

25. Indique qué empresas privadas, consultoras, universidades, laboratorios tecnológicos o proveedores participan o participarían del diseño, desarrollo, implementación, mantenimiento, auditoría o entrenamiento del sistema.

26. Informe si se realizaron procesos de licitación pública o si las contrataciones fueron efectuadas mediante mecanismos de contratación directa, precisando fundamento normativo y procedimiento aplicado en cada caso.

27. Precise si existen acuerdos, convenios o negociaciones con empresas extranjeras vinculadas al desarrollo de herramientas de inteligencia artificial aplicadas a funciones estatales.

28. Informe si el sistema contempla mecanismos de auditoría externa independiente respecto del funcionamiento algorítmico, procesamiento de datos y resultados producidos.

29. Precise si el código fuente, arquitectura técnica, modelos utilizados y criterios de funcionamiento podrán ser auditados por organismos públicos de control, universidades, organismos independientes o el Congreso de la Nación.

30. Indique qué medidas se adoptarán para prevenir discriminación algorítmica, sesgos automatizados, decisiones arbitrarias, falsos positivos, utilización indebida de datos sensibles, vulneraciones a la privacidad o afectaciones a derechos fundamentales.

31. Informe si se realizaron evaluaciones de impacto en derechos humanos, privacidad, protección de datos personales, no discriminación o transparencia institucional antes de la implementación o puesta en funcionamiento del sistema.

32. En caso afirmativo, remita copia íntegra de dichas evaluaciones y precise qué organismos, universidades, consultoras o equipos técnicos las realizaron.

33. Informe si intervino la Agencia de Acceso a la Información Pública, la Dirección Nacional de Protección de Datos Personales o cualquier otro organismo con competencia específica en la materia.

34. Indique qué mecanismos tendrán los ciudadanos para:

    a. conocer qué datos posee el sistema sobre ellos;
    b. solicitar rectificación o actualización;
    c. requerir supresión de información;
    d. impugnar decisiones automatizadas;
    e. acceder a revisión humana de resultados producidos por sistemas algorítmicos;
    f. conocer criterios de clasificación o segmentación eventualmente utilizados.

35. Informe si el sistema contempla participación, intervención, acceso o utilización por parte de organismos de seguridad, fuerzas federales, organismos de inteligencia o estructuras vinculadas al Sistema de Inteligencia Nacional.

36. Precise si el sistema podrá ser utilizado con fines de monitoreo social, vigilancia, prevención, trazabilidad poblacional, análisis conductual o elaboración de perfiles ciudadanos.

37. Informe si se prevé la utilización del sistema en áreas vinculadas a seguridad pública, asistencia social, salud, educación, asignación de prestaciones, prevención del delito, administración de beneficios estatales, análisis electoral o comportamiento ciudadano.

38. Informe qué mecanismos de supervisión parlamentaria, auditoría institucional y control democrático fueron previstos respecto del funcionamiento del sistema.

39. Precise si el Poder Ejecutivo Nacional prevé impulsar un marco regulatorio específico para el uso estatal de sistemas de inteligencia artificial y procesamiento masivo de datos.

40. Informe si se evaluó la compatibilidad del sistema con:

    a. la Constitución Nacional;
    b. la Ley N° 25.326 de Protección de Datos Personales;
    c. la Ley N° 27.275 de Acceso a la Información Pública;
    d. los estándares de la Corte Interamericana de Derechos Humanos;
    e. la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO;
    f. la Resolución 78/265 de la Asamblea General de Naciones Unidas;
    g. el Reglamento Europeo de Inteligencia Artificial (AI Act).

41. Informe si se prevén mecanismos de participación ciudadana, consulta pública o audiencias públicas previas respecto de la implementación de este tipo de tecnologías por parte del Estado Nacional.

42. Remita toda otra información que considere relevante para el adecuado control parlamentario de sistemas de inteligencia artificial, modelización predictiva y construcción de "gemelos digitales" aplicados a funciones estatales.

Pablo JULIANO
Gisella SCAGLIA
Esteban PAULÓN
Alejandra TORRES
Carolina BASUALDO

FUNDAMENTOS

Señor Presidente:

En el transcurso del año 2025, funcionarios del Poder Ejecutivo Nacional anunciaron públicamente el desarrollo e implementación de sistemas de inteligencia artificial (IA), modelización predictiva e interoperabilidad masiva de bases de datos bajo la denominación de "gemelo digital social". Según las manifestaciones públicas realizadas, el sistema tendería a integrar datos provenientes de múltiples organismos del Estado Nacional —ANSES, AFIP/ARCA, PAMI, RENAPER y otros— con el objeto de modelizar comportamientos sociales, simular escenarios de política pública y orientar decisiones de gobierno.

La relevancia institucional de este anuncio no puede subestimarse. Lo que se describe es, en términos de la clasificación establecida por el Reglamento Europeo de Inteligencia Artificial (AI Act), un sistema de "alto riesgo": un dispositivo tecnológico que interviene en decisiones públicas que afectan derechos fundamentales, que procesa datos personales sensibles a escala masiva y que opera sobre la base de modelos matemáticos cuyo funcionamiento interno resulta opaco para los ciudadanos y para las instituciones de control. La calificación de "alto riesgo" no es retórica: determina, en el derecho comparado, un régimen diferenciado de obligaciones, controles previos y estándares de transparencia que el Estado argentino no puede ignorar sin consecuencias constitucionales.

La presente declaración no expresa una posición de principio contra la modernización tecnológica del Estado. Expresa, en cambio, la exigencia republicana y constitucional de que esa modernización se produzca dentro del Estado de Derecho y no al margen de él. Esa exigencia tiene nombre jurídico preciso: legalidad, transparencia, proporcionalidad, control democrático y garantía efectiva de derechos.

La doctrina constitucional argentina, siguiendo la elaboración pionera del Tribunal Constitucional Federal alemán en el "Fallo del Censo" (Volkzählungsurteil, BVerfGE 65, 1, 1983), reconoce la autodeterminación informativa como un derecho fundamental autónomo: la facultad del individuo de decidir, en principio, cuándo y dentro de qué límites sus datos personales pueden ser procesados por terceros. El Tribunal alemán sostuvo que quien no puede saber con certeza qué información existe sobre él y quién la conoce, no puede ser considerado libre en el pleno sentido del término.

Esta construcción dogmática fue recepcionada en el derecho constitucional argentino a través del artículo 43, tercer párrafo, de la Constitución Nacional, que incorporó el hábeas data como garantía constitucional específica. La Corte Suprema de Justicia de la Nación, en el precedente "Cadius c/ Cámara Electoral Nacional" (Fallos 335:252, 2012), reconoció que el hábeas data tutela no solo el acceso a los datos, sino el derecho sustantivo a controlar el uso que el Estado hace de la información personal. Un sistema que integra masivamente datos de ciudadanos sin su conocimiento ni

consentimiento vulnera este núcleo constitucional con independencia de los fines declarados que lo justifiquen.

La protección constitucional de la autodeterminación informativa adquiere una dimensión especialmente crítica cuando el tratamiento de datos es realizado por el propio Estado. A diferencia de los actores privados, el Estado posee poder coactivo y acceso cuasimonopólico a datos sensibles obtenidos por vía de obligaciones legales —declaraciones impositivas, registros previsionales, padrones electorales, historias clínicas en hospitales públicos—. El ciudadano que proporcionó esos datos al Estado en el marco de relaciones jurídicas específicas y con finalidades determinadas tiene un interés constitucionalmente protegido en que no sean utilizados para finalidades distintas sin habilitación legal expresa.

El artículo 19 in fine de la Constitución Nacional establece el principio de legalidad formal: ningún habitante puede ser privado de sus derechos sino en virtud de ley. Este principio, en su versión reforzada aplicable a derechos fundamentales, exige que las restricciones a esos derechos sean establecidas por el Poder Legislativo mediante ley formal, con suficiente densidad normativa para determinar los elementos esenciales del régimen jurídico aplicable.

La Corte Interamericana de Derechos Humanos elaboró esta exigencia de manera sistemática en su Opinión Consultiva OC-6/86 ("Expresiones Ley y leyes en el artículo 30 de la CADH"), estableciendo que la expresión "ley" en el sistema interamericano se refiere a norma jurídica de carácter general emanada del órgano legislativo constitucionalmente previsto, dictada conforme al procedimiento establecido, y que el acto normativo emanado del Poder Ejecutivo —decretos, resoluciones, actos administrativos— no satisface el estándar de "previsión legal" requerido para restringir derechos convencionales.

La implementación de un sistema de IA que procesa masivamente datos personales de ciudadanos argentinos con impacto en el diseño de políticas públicas constituye, en términos estrictamente jurídicos, una restricción al derecho a la autodeterminación informativa, a la privacidad y a la no discriminación. Como tal, requiere habilitación legislativa previa, específica y suficiente. No puede ser implementada por decreto ni por acto administrativo de ningún rango, sin incurrir en una usurpación de las atribuciones propias del Poder Legislativo que viola el principio de división de poderes del artículo 1° de la Constitución Nacional.

La Corte Suprema de Justicia de la Nación, en el precedente "Mazzeo" (Fallos 330:3248, 2007), incorporó expresamente la doctrina del control de convencionalidad elaborada por la Corte IDH, estableciendo que los jueces y demás órganos del Estado argentino están obligados a aplicar la Convención Americana sobre Derechos Humanos y la jurisprudencia interamericana, dejando sin efecto las normas internas que resulten incompatibles con esos estándares. Este mandato no se limita al Poder Judicial: alcanza a todos los órganos del Estado, incluyendo al Poder Ejecutivo en el ejercicio de sus atribuciones administrativas.

La Corte IDH estableció en "Mejoría Idosa y Otros vs. México" (2021) y en los estándares sobre "Tecnologías digitales y derechos humanos" publicados por la CIDH en 2023 que el uso de sistemas de IA por parte del Estado que pueda derivar en vigilancia masiva, discriminación o restricciones no proporcionales a derechos fundamentales debe estar sujeto a control judicial efectivo, regulación legal previa y mecanismos de rendición de cuentas. La ausencia de esos controles constituye una violación convencional que compromete la responsabilidad internacional del Estado argentino.

Los artículos 16 y 75 inciso 23 de la Constitución Nacional consagran el principio de igualdad y la obligación del Estado de adoptar medidas de acción positiva que remuevan obstinaciones discriminatorias estructurales. La paradoja que plantean los sistemas de IA es que pueden producir discriminación estructural precisamente bajo la apariencia de objetividad científica.

La discriminación algorítmica ha sido documentada en múltiples jurisdicciones y estudios empíricos. El caso paradigmático es COMPAS, un algoritmo de evaluación de riesgo de reincidencia utilizado en el sistema judicial estadounidense que fue analizado por ProPublica en 2016 y demostró una tasa de falsos positivos significativamente mayor para imputados afrodescendientes que para imputados blancos. En el campo de las políticas sociales, el "Fragile Families Challenge" (Princeton, 2020) concluyó que los modelos predictivos aplicados a políticas de protección de la infancia reproducen sistemáticamente sesgos de clase y raza. En Argentina, la ausencia de estándares obligatorios de evaluación de impacto discriminatorio antes de la implementación de sistemas de IA en el sector público hace que este riesgo sea de especial gravedad institucional.

La Ley N° 25.326 de Protección de Datos Personales establece en su artículo 4°, inciso 3°, que los datos deben ser recolectados para "finalidades determinadas, explícitas y legítimas" y que no deben ser tratados de manera "incompatible con dichas finalidades". Este principio —conocido en el derecho comparado como "purpose limitation"— constituye uno de los pilares más importantes de la arquitectura legal de protección de datos y su violación potencial en el contexto del "gemelo digital social" es directa e inmediata.

Los datos que el Estado obtiene de los ciudadanos a través de ANSES (con la finalidad de gestionar prestaciones previsionales), de AFIP/ARCA (con la finalidad de recaudar tributos), del RENAPER (con la finalidad de identificar personas), o del padrón electoral (con la finalidad de organizar el sufragio) fueron provistos por los titulares en el marco de obligaciones legales específicas y con finalidades jurídicamente delimitadas. Su utilización combinada e integrada para alimentar modelos predictivos de políticas públicas constituye, en principio, un uso incompatible con las finalidades originarias, que requiere habilitación legal expresa y, en la mayoría de los casos, mecanismos de información al titular de los datos.

La Dirección Nacional de Protección de Datos Personales (DNPDP), en su carácter de autoridad de aplicación, tiene facultades expresas de fiscalización y sanción frente a violaciones de estos

principios. Sin embargo, y esto constituye uno de los problemas estructurales que la presente declaración busca visibilizar, la DNPDP carece actualmente de los recursos técnicos, humanos e institucionales necesarios para auditar sistemas de IA de la complejidad del que se anuncia. La Ley N° 25.326 fue sancionada en el año 2000, antes de la emergencia de los sistemas de aprendizaje automático a escala masiva, y su régimen no contempla expresamente la regulación de sistemas algorítmicos autónomos. Esta brecha regulatoria es, precisamente, uno de los argumentos más sólidos en favor de la necesidad de legislación específica.

La Ley N° 27.275 de Acceso a la Información Pública establece en su artículo 1° que toda persona tiene derecho a solicitar y recibir información completa, veraz, adecuada y oportuna del sector público, y consagra en su artículo 3° el principio de máxima divulgación, conforme al cual toda restricción a ese derecho debe ser interpretada con carácter restrictivo. La ley incluye expresamente como sujetos obligados a todos los órganos del Poder Ejecutivo Nacional.

La transparencia algorítmica —el derecho a conocer cómo funcionan los sistemas automatizados que intervienen en decisiones públicas— es una derivación directa del derecho de acceso a la información pública tal como ha sido interpretado por la Agencia de Acceso a la Información Pública (AAIP) y por la doctrina especializada. El código fuente de un sistema de IA utilizado para diseñar políticas públicas, los datos de entrenamiento empleados, las metodologías de validación y los criterios de funcionamiento del modelo constituyen información de carácter público que el Estado tiene la obligación de divulgar, salvo que pueda acreditar una excepción de las taxativamente previstas en la ley.

La Ley N° 25.520 de Inteligencia Nacional y su modificatoria, la Ley N° 27.482, establecen un régimen expreso de prohibiciones orientado a prevenir el uso de capacidades de inteligencia del Estado contra la propia ciudadanía. El artículo 4° de la Ley N° 25.520 prohíbe expresamente a los organismos de inteligencia "producir inteligencia interior" sobre ciudadanos argentinos en base a su "raza, fe religiosa, acciones privadas, u opinión política", salvo en el marco de una investigación criminal autorizada por autoridad judicial competente.

Un sistema de IA que produce perfiles ciudadanos, predicciones de comportamiento social y segmentaciones poblacionales sobre la base de la integración masiva de datos del Estado puede operar, desde una perspectiva funcional, como un sistema de inteligencia interior sin las salvaguardas que la Ley N° 25.520 establece para esas actividades. La falta de claridad sobre la separación institucional entre los organismos que operarían el "gemelo digital social" y los organismos de inteligencia del Estado —y especialmente la ausencia de garantías de que el acceso de los últimos al primero esté prohibido y sea auditable— constituye uno de los aspectos de mayor gravedad institucional que justifica el presente pedido de informes.

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), incorporado al bloque de constitucionalidad federal por el artículo 75, inciso 22, de la Constitución Nacional, establece que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada. El Comité

de Derechos Humanos de Naciones Unidas, en su Observación General N° 16 (1988), interpretó que esta disposición impone al Estado la obligación de contar con legislación que regule el almacenamiento y uso de datos personales, garantice la finalidad legítima del tratamiento y establezca mecanismos efectivos de control.

En 2021, el mismo Comité, en sus "Directrices sobre privacidad digital", expresó que los principios del artículo 17 se aplican plenamente al procesamiento automático de datos en entornos digitales y que el carácter masivo del procesamiento, la sofisticación de los modelos algorítmicos y el potencial de uso combinado de datos —el llamado "combinatorial effect"— agravan el riesgo de injerencia arbitraria y refuerzan las obligaciones de los Estados en materia de protección legislativa.

La Resolución 78/265 de la Asamblea General de Naciones Unidas (2024), sobre "Inteligencia artificial segura, protegida y confiable", constituye el primer documento de consenso universal en la materia. Sus parámetros centrales —gobernanza centrada en derechos humanos, transparencia, responsabilidad, supervisión humana y acceso a recurso efectivo— configuran un estándar internacional que los Estados deben tomar como referencia mínima.

La Comisión Interamericana de Derechos Humanos publicó en octubre de 2023 su Informe "Inteligencia Artificial y Derechos Humanos" (OEA/Ser.L/V/II, Doc. 196/23), el documento de mayor especificidad producido hasta el presente en el sistema regional. El informe establece que los sistemas de IA utilizados por Estados en el diseño de políticas públicas son compatibles con la Convención Americana sobre Derechos Humanos únicamente cuando se verifican, de manera acumulativa, las siguientes condiciones: (a) base legal suficientemente precisa para ser previsible; (b) finalidad legítima y necesaria en una sociedad democrática; (c) proporcionalidad estricta; (d) evaluación de impacto previa; (e) supervisión humana efectiva; (f) mecanismos de recurso accesibles; y (g) rendición de cuentas institucional.

Ningún sistema que no satisfaga todas y cada una de estas condiciones puede ser calificado como compatible con el estándar convencional. La ausencia de información pública suficiente sobre el "gemelo digital social" impide determinar si estas condiciones se encuentran cumplidas, lo que en sí mismo constituye un incumplimiento del requisito de previsibilidad legal y transparencia que la Convención impone.

La Recomendación sobre la Ética de la Inteligencia Artificial, adoptada por consenso en la 41ª Conferencia General de la UNESCO el 23 de noviembre de 2021, con el voto favorable de la República Argentina, es el primer instrumento normativo global de carácter integral sobre IA. Si bien no es un tratado vinculante, genera obligaciones de buena fe en materia de implementación y configura un estándar internacional de referencia con plena relevancia hermenméutica para la interpretación del bloque de constitucionalidad federal.

La Recomendación establece en su Sección IV, dedicada a los valores y principios, que los sistemas de IA que intervengan en decisiones con impacto en derechos humanos deben someterse

a "evaluaciones de impacto sobre derechos humanos" (Human Rights Impact Assessments) antes de su implementación y de manera periódica durante su funcionamiento. Establece también que los Estados deben garantizar el "derecho a no ser sometido a decisiones determinadas exclusivamente por procesos automatizados" cuando esas decisiones afecten derechos fundamentales. Ambos principios son de aplicación directa al caso que nos ocupa.

El Reglamento de la Unión Europea 2024/1689, conocido como AI Act, entró en vigor el 1° de agosto de 2024 y es aplicable de manera progresiva hasta agosto de 2026. Constituye el instrumento de regulación de IA de mayor madurez y detalle técnico disponible a nivel global y sus estándares son ampliamente utilizados en el derecho comparado como referencia normativa, incluso fuera del ámbito de la Unión Europea.

Para los propósitos de la presente declaración, tres aspectos del AI Act merecen especial consideración:

- **Sistemas prohibidos:** El artículo 5 del AI Act prohíbe expresamente los "sistemas de puntuación social" (social scoring) utilizados por autoridades públicas para evaluar o clasificar a personas o grupos en función de comportamientos o características personales. La prohibición alcanza a los sistemas que producen perjuicios desproporcionados o injustificados en contextos no relacionados con aquél en que se generaron los datos. Un sistema de modelización predictiva que segmenta a la ciudadanía por comportamientos sociales para orientar políticas públicas puede quedar comprendido en esta categoría prohibida.
- **Sistemas de alto riesgo:** El Anexo III del AI Act clasifica como "alto riesgo" a los sistemas de IA utilizados en "gestión y operación de infraestructura crítica", "acceso a prestaciones y servicios públicos esenciales" y "evaluación y clasificación de personas físicas para acceder a servicios públicos". Estos sistemas están sujetos a: evaluación de conformidad previa, registro en bases de datos públicas de la UE, supervisión humana obligatoria, documentación técnica exhaustiva, trazabilidad de decisiones y mecanismos de recurso.
- **Obligaciones de transparencia:** El artículo 13 del AI Act exige que los sistemas de alto riesgo sean diseñados de manera que permitan a los usuarios comprender los resultados del sistema ("explicabilidad") y detectar y corregir errores. Esta obligación de explicabilidad es uno de los desafíos técnicos más complejos en sistemas de aprendizaje profundo, precisamente por la naturaleza de "caja negra" de los modelos de alta complejidad.

La Directiva canadiense sobre Decisión Automatizada (2019, revisada en 2023) establece un sistema de cuatro niveles de riesgo para sistemas de IA utilizados por el Gobierno Federal. Para los sistemas de nivel 3 y 4 —aquellos con impacto significativo sobre derechos individuales o colectivos— exige: evaluación de impacto algorítmico obligatoria previa a la implementación, publicación de los resultados de esa evaluación, explicación comprensible de las decisiones automatizadas a los ciudadanos afectados, revisión humana obligatoria de las decisiones de mayor impacto, y auditoría periódica por el Comisionado de Privacidad.

El modelo canadiense es relevante porque demuestra que la regulación efectiva de IA en el sector público no requiere prohibiciones generales sino marcos diferenciados que calibren las obligaciones en función del riesgo concreto. Es, en ese sentido, un modelo de regulación habilitante y proporcional que la República Argentina podría tomar como referencia positiva en la elaboración de su propio marco normativo.

La Lei Geral de Proteção de Dados Pessoais (LGPD, Ley N° 13.709/2018) establece en su artículo 20 el derecho de todo titular a solicitar "revião de decisões tomadas únicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses". La LGPD exige que el responsable del tratamiento informe al titular sobre la lógica y los criterios utilizados en el procesamiento automatizado. En su artículo 20, inciso 3°, la ley dispone que el controlador debe informar de manera clara y adecuada los critérios e procedimentos utilizados para a decisão automatizada.

La Autoridade Nacional de Proteção de Dados (ANPD) de Brasil ha avanzado significativamente en la interpretación de estas normas en el contexto de sistemas de IA utilizados por el sector público, emitiendo en 2023 orientaciones específicas sobre los requisitos de transparencia y rendición de cuentas aplicables a sistemas de toma de decisiones automatizadas en políticas públicas. La experiencia regulatoria brasileña es especialmente relevante para la Argentina por la cercanía cultural, jurídica e institucional entre ambos países.

El Consejo de Estado de Colombia emitió en 2022 (Expediente N° 11001-03-15-000-2021-02398-01) una sentencia de carácter fundacional en materia de transparencia algorítmica. En ese fallo, el máximo tribunal de lo contencioso administrativo colombiano estableció que los ciudadanos tienen derecho a conocer los criterios y ponderaciones utilizados en sistemas algorítmicos utilizados por el Estado para adoptar decisiones que los afecten, y que la negativa de la administración a revelar esa información bajo el argumento de secreto comercial o confidencialidad tecnológica es incompatible con los principios de publicidad y transparencia que rigen la función pública. Este precedente, dictado en el marco de un sistema jurídico de derecho civil con numerosas coincidencias con el argentino, tiene particular relevancia comparada.

El Convenio 108+ del Consejo de Europa —actualizado en 2018 para adaptarse al entorno digital— y la Recomendación CM/Rec(2020)1 sobre "Impactos en derechos humanos del procesamiento algorítmico" constituyen los instrumentos de derecho convencional internacional más específicos en la materia. La Recomendación CM/Rec(2020)1, no siendo un tratado vinculante, expresa el consenso de los cuarenta y seis Estados del Consejo de Europa y establece parámetros de interés hermenméutico universal: la necesidad de "aucitorias de impacto" previas, la exigencia de "documentación técnica" accesible para los reguladores, y el principio de "supervisor humano significativo" —no meramente formal— para los sistemas de IA con impacto en derechos fundamentales.

La implementación de sistemas de IA en el sector público plantea una dimensión que trasciende la protección individual de datos y alcanza la soberanía del Estado sobre su propia información estratégica. Un "gemelo digital social" que modela la estructura social, económica y demográfica de la República Argentina constituye, desde la perspectiva de la seguridad nacional y la soberanía informática, un activo estratégico de primer orden.

Las preguntas fundamentales que ningún instrumento público ha respondido hasta el presente son: ¿dónde se almacenan físicamente los datos? ¿En servidores bajo soberanía argentina o en infraestructura en la nube de proveedores extranjeros? ¿Bajo qué legislación quedan regidos los datos en caso de conflicto con el proveedor? ¿Puede el Estado argentino acceder a sus propios datos si el contrato con el proveedor privado se rescinde? La respuesta a estas preguntas determina si la soberanía informacional del Estado argentino sobre sus propios datos permanece integra o es cedida, de hecho, a actores privados extranjeros bajo contratos de adhesión cuyas condiciones no son públicamente conocidas.

El artículo 75, inciso 8°, de la Constitución Nacional atribuye al Congreso la facultad exclusiva de fijar anualmente el presupuesto general de gastos y recursos de la administración nacional. Esta atribución no es meramente formal: constituye el principal instrumento de control parlamentario sobre las políticas públicas del Poder Ejecutivo. Un gasto no previsto en el presupuesto o financiado mediante reasignación discrecional de partidas por parte del Ejecutivo, sin conocimiento ni autorización del Congreso, plantea una cuestión constitucional de primera magnitud.

La posible participación de organismos multilaterales de crédito —Banco Interamericano de Desarrollo, Banco Mundial— en el financiamiento del sistema agrega una capa adicional de complejidad: los préstamos multilaterales generan condicionalidades, compromisos de política pública y obligaciones jurídicas internacionales que el Congreso tiene derecho a conocer, dado que pueden comprometer el presupuesto nacional a futuro y condicionar la capacidad de decisión del Estado sobre el propio sistema.

Uno de los riesgos institucionales menos visibles pero de mayor gravedad estructural en los proyectos de tecnología pública desarrollados por actores privados es el denominado "vendor lock-in": la situación en que el Estado queda tecnológicamente dependiente de un proveedor específico porque los datos, el código fuente, los modelos entrenados o la arquitectura del sistema son de titularidad del proveedor y no del Estado. En este escenario, la rescisión del contrato puede implicar la pérdida de acceso al sistema y a los datos procesados, convirtiendo al proveedor privado en un actor con poder de negociación desproporcionado frente al Estado.

Los principios jurídicos de inalienabilidad de los bienes del dominio público del Estado y la doctrina constitucional sobre la interdicción de la privatización de funciones estatales esenciales imponen que, cuando el Estado encarga a un privado el desarrollo de sistemas tecnológicos destinados a ejercer funciones públicas, la titularidad sobre el código, los datos y los modelos debe

corresponder al Estado o, al menos, estar garantizado contractualmente el acceso irrestricto del Estado a esos activos en cualquier circunstancia.

La frontera entre un sistema de IA orientado al diseño de políticas públicas y un sistema de vigilancia social masiva no es tecnológica sino institucional. Depende, exclusivamente, de las decisiones políticas sobre su gobernanza, sus finalidades permitidas, sus restricciones de acceso y sus mecanismos de control. En ausencia de esas definiciones institucionales —que hoy no existen en el derecho positivo argentino—, la misma infraestructura técnica puede ser utilizada para ambos propósitos.

La experiencia comparada es ilústrativa y alarmante. El sistema chino de "rédito social", construido sobre una infraestructura de integración de bases de datos gubernamentales que en sus orígenes se justificó como herramienta de política pública, derivó en un mecanismo de vigilancia y control social masivo. El programa PRISM de los Estados Unidos, revelado por Edward Snowden en 2013, demuestra que incluso en democracias consolidadas la capacidad técnica de procesar masivamente datos ciudadanos es susceptible de ser desviada hacia finalidades de vigilancia sin que existan controles institucionales suficientemente sólidos para impedirlo.

La Argentina tiene una historia institucional que otorga particular sensibilidad a este riesgo. Durante el último gobierno militar, los organismos de inteligencia del Estado utilizaron archivos y bases de datos para perseguir, identificar y desaparecer ciudadanos. Ese pasado impone una responsabilidad histórica y constitucional especial al Estado argentino en materia de diseño de sistemas de integración masiva de datos con capacidad de perfilamiento ciudadano. Las garantías institucionales no son excesos burocráticos: son las lecciones que la historia le imponé al Estado de Derecho.

Del análisis precedente se desprende que la implementación constitucionalmente válida de sistemas de IA aplicados al diseño de políticas públicas en Argentina requiere, como condiciones sine qua non:

- Habilitación legislativa expresa, específica y suficiente: el Congreso Nacional debe sancionar una ley que establezca el régimen jurídico aplicable, defina las finalidades autorizadas, determine los tipos de datos que pueden ser utilizados y establezca las restricciones y controles correspondientes. Ningún decreto ni acto administrativo puede suplir esta exigencia constitucional.

- Evaluación de impacto previa obligatoria: antes de la implementación de cualquier sistema de IA con potencial afectación de derechos fundamentales, debe realizarse una evaluación de impacto sobre derechos humanos, privacidad y discriminación, cuyos resultados deben ser públicos y estar sujetos a control parlamentario.

- Transparencia algorítmica efectiva: el código fuente, los datos de entrenamiento, la arquitectura del modelo, los parámetros de funcionamiento y los resultados de las auditorías

deben estar disponibles para los organismos públicos de control, el Poder Legislativo y, en la medida compatible con la protección de datos de terceros, la ciudadanía en general.

- Supervisión humana significativa: las decisiones de política pública que sean orientadas o influidas por el sistema no pueden adoptarse sin intervención humana responsable y trazable. La responsabilidad política y jurídica del Estado no puede ser delegada en un algoritmo.

- Garantías de soberanía tecnológica: los datos deben almacenarse en servidores bajo jurisdicción argentina, el Estado debe ser titular del código y los modelos, y los contratos con proveedores privados deben garantizar la continuidad del acceso estatal en cualquier escenario de rescisión contractual.

- Separación efectiva respecto de organismos de inteligencia: debe garantizarse mediante norma expresa y mecanismo de control auditable que los organismos de inteligencia del Estado no tienen acceso al sistema ni a sus datos, sin perjuicio de lo que autoricen las leyes específicas con control judicial.

- Control democrático parlamentario: el Congreso Nacional debe contar con información suficiente, oportuna y auditable sobre el funcionamiento del sistema, con facultades efectivas de supervisión y con mecanismos de sanción ante incumplimientos.

- Mecanismos de recurso efectivos para los ciudadanos: toda persona que sea objeto de una decisión de política pública que haya sido influida por el sistema debe tener derecho a conocer ese hecho, a obtener una explicación comprensible de los criterios aplicados y a impugnar la decisión ante una autoridad humana competente.

La Historia del constitucionalismo moderno puede leerse como la historia de los esfuerzos institucionales de las sociedades por acotar, controlar y hacer rendir cuentas al poder. Cada nueva forma de poder —económico, militar, informático— ha planteado el mismo desafío: cómo incorporar esa nueva forma de poder al espacio del Derecho, sin extinguir su capacidad transformadora pero sin permitir que operen fuera de los límites constitucionales.

El poder algorítmico del Estado —la capacidad de procesar masivamente datos ciudadanos, producir predicciones de comportamiento social y orientar decisiones de política pública mediante sistemas automáticos— es la nueva forma de poder que el constitucionalismo del siglo XXI debe aprender a controlar. No es un desafío técnico. Es un desafío institucional y democrático de primera magnitud.

El presente pedido de informes es, en ese sentido, una afirmación del rol irreemplazable del Poder Legislativo en ese proceso. La Honorable Cámara de Diputados de la Nación no interpela al Poder Ejecutivo como obstáculo a la modernización: lo interpela como garante de la constitucionalidad del ejercicio del poder estatal. Esa interpelación es, en sí misma, el ejercicio de la función de

control democrático que la Constitución le atribuye al Poder Legislativo como misión esencial e indelegable.

Un Estado que implementa sistemas de inteligencia artificial sin ley habilitante, sin evaluación de impacto, sin transparencia, sin control democrático y sin garantías de soberanía tecnológica no es un Estado moderno: es un Estado que ha elegido la opacidad sobre la legalidad. Y la opacidad del poder —como enseña la experiencia argentina y universal— es siempre el primer paso hacia su abuso.

Por las razones constitucionales, legales, convencionales y de derecho comparado expuestas, solicito a mis pares el acompañamiento del presente proyecto de resolución

Pablo JULIANO
Gisella SCAGLIA
Esteban PAULÓN
Alejandra TORRES
Carolina BASUALDO