Bases para un Observatorio de uso de Inteligencia Artificial en el Estado
Informe de la 2da Reunión realizada el 23/08/2022

Introducción

En el marco de la implementación del compromiso 1.6 del 5to Plan de Acción Nacional de Gobierno Abierto, que tiene por objetivo la creación de un Observatorio de uso de Inteligencia Artificial en el Estado [1] que promueva y fomente el uso ético, responsable, seguro y confiable de esta tecnología, y que fortalezca el ecosistema de inteligencia artificial en Uruguay; se desarrolló la 2da. Reunión de intercambio el pasado 23 de agosto de 2022.

El objetivo de esta nueva instancia fue continuar con los espacios de intercambio para recabar propuestas, y conocer las temáticas, problemas y desafíos que en cada sector se identifican para avanzar en insumos de las metas del compromiso que, en esta ocasión, se focalizó en:

- Cómo integrar transparencia y acceso a la información pública a la temática de algoritmos e inteligencia artificial.

  Meta: "*Desarrollar criterios y recomendaciones para las Instituciones públicas que den pautas para la transparencia de algoritmos en las aplicaciones de uso de IA en el Estado, en sinergia con la normativa vigente en materia de Transparencia y Acceso a la Información Pública*" y

- Cuáles serían los usos de IA por parte del Estado que aportarían a la población, además de que los sistemas tengan mitigados los sesgos y sean creados bajo los principios orientadores de transparencia por diseño y de privacidad por diseño.

  Meta: "*Promover el uso de la tecnología de la IA en beneficio de la población contemplando aspectos de ética, privacidad, responsabilidad, transparencia y no discriminación*".

La actividad fue organizada por la Unidad de Acceso a la Información Pública (UAIP) y Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) y de la misma participaron 28 personas de diferentes Instituciones del Estado, de la Academia, de la Sociedad Civil, y del Sector Privado.

[1] *Ver compromiso 1.6 – Observatorio de uso de IA en el Estado - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/5to-plan-accion-nacional-gobierno-abierto-2021-2024/compromisos/1*

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/observatorio-uso-inteligencia-artificial-estado

Se trabajó sobre los mismos ejes propuestos en agenda en 2 grupos en forma simultánea, para favorecer la participación de todos los asistentes y escuchar la mayor cantidad de aportes y propuestas. Luego se hizo una puesta en común de las principales ideas surgidas.

Este documento presenta un resumen de los aportes recibidos en el marco de la 2da Reunión de intercambio "Bases para un Observatorio de uso de Inteligencia Artificial en el Estado".

Detalles de los aportes recibidos

Los aportes recibidos durante el intercambio abarcaron varios puntos relacionados con la transparencia algorítmica, el acceso a la información pública, los sesgos y algunos temas que acceden a la temática propuesta.

La sistematización que se presenta a continuación identifica los aspectos que las y los participantes consideraron deberían ser abordados:

a) Transparencia algorítmica – diferentes pautas de qué y cómo transparentar.
b) Publicación y comunicación considerando diferentes públicos objetivo, contenidos, etc.
c) Otros temas vinculados al objetivo de la reunión, entre otros, referidos a la búsqueda de antecedentes en otros países que están trabajando en la temática, impacto en materia de derechos humanos, beneficios y riesgos.

Transparencia algorítmica

Vinculado a la transparencia algorítmica en casos de aplicación de Inteligencia Artificial, se compilaron varias ideas surgidas del intercambio.

- **Los datos.** Transparencia en la entrada de datos más que en el resultado. Garantizar cómo se entrena el algoritmo evitando sesgos, puesto que el resultado es más difícil de explicar. Publicar la explicación del resultado, podría limitar la innovación en el Estado y en la industria con la explicación del resultado.
- **Equilibrio**. Encontrar el equilibrio entre transparentar para técnicos (de tecnología) y para otro público, mostrando el cómo se hizo. Mostrar datos anonimizados cuidando datos personales o protegidos. Se mencionó el ejemplo de simulación del caso de reforma jubilatoria.
- **Código**. Publicar el código puede tener ventajas y desventajas. Se podría publicar un ejemplo de data set y los algoritmos utilizados para visibilizar cómo se usa, y testearlo en ambiente controlado. Se mencionaron ejemplos en aplicaciones financieras y de secreto tributario.
- **Ciberseguridad**. Tomar precauciones sobre qué transparentar. Diferencia entre contenido público, privado y restringido.
- **Privacidad**. Que sea pública la base de datos de entrenamiento depende de los datos con los cuales se trabajó. Hay bases que dependen de la privacidad y otras que deberían estar públicas. Definir hasta dónde se puede dar información y hasta donde no.

- **Objetivo**. Determinar el objetivo respecto a compartir y reutilizar. Podría ser dar respuesta a peticiones o transparentar y disponibilizar. Cumplir con más de un objetivo.
- **Grados.** Incentivar desde el Observatorio IA la transparencia de dónde se usa, qué se usa y el algoritmo que se usa, con grados de apertura según el caso.
- **Gobernanza.** Segmentar qué se presenta a diferentes públicos. Hasta dónde transparentar previa validación, tiene que ver con la gobernanza del sistema, respetando que no se vulneren derechos.
- **Ámbito jurídico.** Principio de equivalencia funcional. Hay cosas que se podrán mostrar y otras que no, asociado a la ciberseguridad. La apertura debería ser relativa a modo de excepción. Se menciona el ejemplo del software del sistema de Cannabis, que no es público.
- **Base de conocimiento de algoritmos.** Cuestión fundamental, asimilable a bases de datos que exista transparencia. Deben estar contenidas las normas de DDHH. Ruta de análisis de la toma de decisiones.
- **Plantilla.** Disponer de una plantilla de información orientada a quien conoce el algoritmo que incluye datos, el para qué, los beneficios, la evolución y el entrenamiento. Materializar el contenido para su publicación.

Publicación

- **Documentación.** Generar documentación orientada a los diferentes públicos objetivo y generar diferentes entregables y formatos: ej. videos, documentos técnicos.
- **Lenguaje**. Comprensible y claro para el común de la ciudadanía.
- **Repositorio**. Buena idea. Repositorio centralizado que podría ser la "Red.uy" de los algoritmos. Presenta desafío respecto a los sesgos. Podrían ser también repositorios sectoriales a considerar.
- **Almacenamiento**. En el territorio nacional. Ej. ANTEL, evitando uso de nubes y hosts de datos fuera del país. Trabajar para que nubes públicas y privadas tengan todas las mismas buenas prácticas. La estrategia de ANTEL es disponibilizar los datos en APIs para su reutilización.
- **Empoderamiento**. Para que Agesic pueda manejar algoritmos con objetivos específicos.
- **Confidencialidad**. Datos privados y datos públicos para analizar dónde compartir cada uno. Estudiar pautas europeas en la materia.
- **Supervisión y Control**. Crear agencias para generar auditorías: a) para asegurar calidad de datos evitando sesgos y errores en la toma de decisiones, b) por temas de ética generando confianza en la ciudadanía con el uso de IA, c) generando autoconfianza.
- **Cómo publicar**. Utilizar medios legales, tales como sitios web y otras herramientas para ampliar alcance.
- **Cuándo publicar**. Definir si se publica antes o después de la aplicación.
- **Control de calidad**. Tener instrucciones sobre cómo se genera la información para que sea confiable. Pensar en el usuario final de la información.
- **Modificaciones**. Los algoritmos son organismos vivos, que se van transformando. En instancias puntuales de llamados, debería considerarse en las bases, referencias concretas y vigentes.

- **Documentos internos**. Manejar pautas internas de clasificación de la información en tanto reservada o no reservada. Ver el nivel crítico de la información.

Sesgos

- **Representatividad**. Adecuada selección de la muestra para cada grupo que se va a incluir. Investigar antecedentes en otros países. No dejar de lado ninguna experiencia de vida.
- **No usar datos no necesarios**. Reducir datos e ignorar los datos que no aportan y además deben de estar anonimizados.

Otros aspectos vinculados

- **Beneficio**. Siempre es beneficioso el uso de IA para el Estado y las personas. Ej. caso de fraude en compras públicas. Mostrar lo que se puede hacer con IA. Aplicar en mejora de eficiencia del Estado. Tiene que estar el beneficio asociado a los riesgos.
- **Políticas**. En base a los beneficios se podrían tomar políticas específicas para su uso.
- **Marco**. Habrá beneficio si existe marco operativo previamente controlado y avalado por un Comité, que podría ser el Observatorio IA.
- **Testing**. Debe estar en agenda. Testing de uso y medición de resultados de los algoritmos para recomendar respecto a su fiabilidad.
- **Reglamentación.** Enfoque europeo de recomendaciones para la reglamentación, tiene criterios que vale la pena analizar.
    - **Riesgos.** Enfoque de riesgos claro. Entender los usos de aplicación de IA que tienen mayor y menor riesgo. Análisis de impacto algorítmico en aquellos usos de riesgo alto.
    - **Derechos Humanos.** Dejar mensaje claro de qué usos no admiten la aplicación de IA en el Estado desde el punto de vista de garantía de derechos humanos.
    - **Requisitos.** Tratar en forma diferenciada los requisitos y analizar el costo.
    - **Código de conducta.** Reglas de lo qué se debe informar de forma básica, riesgo medio o bajo
- **Antecedentes e intercambio**. Generar sinergia con países con adelanto en este proceso para ver qué factores se consideraron. Ej. Brasil viene trabajando fuerte a nivel parlamentario. Hay antecedentes también en Chile (que se apoya en antecedentes europeos).
- **Seguimiento**. Analizar en el marco del Observatorio IA, jornadas de seguimiento para generar insumos.
- **Áreas de trabajo**. Analizar niveles de riesgo y generar recomendaciones por áreas y niveles de riesgo. IA y medio ambiente, IA y seguridad, por ejemplo.
- **Relevamiento**. Relevar la realidad uruguaya desde perspectivas de riesgo y áreas de trabajo.
- **Sistema Experticia (Argentina)**. Se trae como ejemplo para apoyar el acceso al algoritmo para dar garantías del debido proceso en materia penal. En materia de DDHH debe disponerse del instrumento para conocer el código fuente y ver qué medidas tomar.

Conclusiones

Después del segundo intercambio, se ha puesto en manifiesto la importancia de seguir trabajando sobre la explicabilidad de los algoritmos en tanto qué, cómo, cuándo, dónde y para quiénes publicar información, considerando aspectos de ciberseguridad, derechos humanos, normativa de protección de datos, y potenciando el desarrollo del Estado y el desarrollo productivo a través del uso de IA. Además, se destacó la importancia de aspectos como almacenamiento, supervisión y control.

Asimismo, se mencionó la necesidad de revisar antecedentes y avances en otros países, aprovechando la participación de Uruguay en diferentes ámbitos internacionales en esta materia.