



Contribución al documento "Recomendaciones para el tratamiento de datos personales en la inteligencia artificial" de la Red Iberoamericana de Protección de Datos (RIPD)

Las firmantes son organizaciones de la sociedad civil que trabajan en la defensa de los derechos humanos en el ámbito digital. Debido a que en varios casos los sistemas de Inteligencia Artificial (IA) usan datos personales para su funcionamiento, cuestiones de privacidad, seguridad y otros derechos merecen la máxima consideración. De lo contrario, existe el riesgo de un abuso de este tipo de tecnologías que conlleven un perjuicio para los derechos humanos de las personas.

En este sentido, valoramos la iniciativa llevada a cabo por la RIPD de contribuir al establecimiento de guías de conducta para los actores responsables de crear, diseñar, implementar o poner en funcionamiento sistemas de IA. De la misma manera, reconocemos la disposición a abrir el documento a consulta para que otros actores puedan ofrecer sus puntos de vista con el fin de enriquecer el debate.

Por lo tanto, a continuación brindamos nuestros comentarios a la versión del documento que nos fue enviada. Esperamos que estos aportes puedan ser considerado para la redacción final de las recomendaciones.

1. En la introducción del documento se menciona que la IA "ha estado en la agenda de los Gobiernos, la industria, la academia y las autoridades de protección de datos personales". **Creemos que debe agregarse a las organizaciones de la sociedad civil en esa enumeración.** El impacto de la IA en los derechos humanos viene siendo investigado y analizado por nuestro sector al mismo tiempo que el trabajo realizado por los otros sectores. En consecuencia, es un tema que también está en la agenda de las organizaciones y como tal, debería ser contemplado en el documento.

2. La introducción también menciona que los "datos personales son el combustible de la IA". Si bien la frase sirve para ejemplificar brevemente el papel de los datos personales en el funcionamiento de la IA, puede llevar a identificar erróneamente a los datos personales con un *commodity* más que opera en el mercado. A diferencia de otros insumos con los cuales es comparado habitualmente -en particular, el petróleo- los datos

personales se refieren a información sobre individuos. Por lo tanto, existe una dimensión cualitativa que no está presente en otros casos. El procesamiento de datos personales implica una intervención en acciones, conductas, opiniones, etc. que hacen a la personalidad del individuo. **Esta característica especial del dato personal debería ser enfatizada por el documento para evitar caer en una visión mercantilista del dato.** Finalmente, no todo desarrollo de IA debe involucrar el uso de datos personales. Si es necesario admitir la experimentación con tecnologías, debería favorecerse los casos donde hay pocos o ningún dato personal involucrado.

3. El documento sostiene que la normatividad exige que el tratamiento "esté rodeado de garantías mínimas". Consideramos que debería reformularse la frase para hablar de **"garantías adecuadas"**. Creemos que es mejor esta redacción, ya que brinda más protección para el titular del dato y evita los peligros de que responsables de sistemas de IA justifiquen su tratamiento mediante el cumplimiento de estándares de mínima que no sirvan para comprender la complejidad del fenómeno.

4. El documento sostiene que no existe una fórmula para alcanzar un punto de equilibrio entre innovación, desarrollo, IA y derechos humanos, y que por eso -en la actualidad- solo son admisibles recomendaciones. Sobre este punto, queremos señalar que un riesgo de este enfoque es el de pensar que actualmente no hay obligaciones a cumplir y que los dilemas que surgen deben ser resueltos a través de sistemas normativos no vinculantes, como la ética. En ese sentido, **creemos que el documento debería enfatizar que los derechos humanos son el marco principal a través del cual evaluar los efectos de la IA en las personas.**

5. El documento recomienda que se efectúe una evaluación de impacto en privacidad (PIA por sus siglas en inglés) previo al diseño y desarrollo de productos de IA. **Para complementar esa tarea, creemos que debería hacerse una evaluación de impactos en derechos humanos en general.** Este enfoque permitiría un mayor análisis acerca de otros derechos que pueden verse afectados por el uso de IA, como el derecho a no sufrir discriminación, derecho al trabajo, derecho a acceder a bienes sociales (salud, educación, etc.) entre otros.

6. **El documento debería contemplar el hecho de que algunos desarrollos de la IA pueden tener efectos particularmente adversos en grupos en situación de vulnerabilidad.** Esta característica resulta relevante en una región con graves niveles de desigualdad como América Latina y el

Caribe. Los sistemas de IA pueden ser utilizados para asignar calificaciones crediticias, predecir zonas donde serán cometidos delitos o decidir quién ocupará un puesto de trabajo, entre otras actividades que impactan en derechos humanos. Si los algoritmos presentan sesgos que refuerzan prejuicios sociales, se corre el riesgo de producir resultados injustos y generar privilegios que incrementan las desventajas sufridas por esos grupos. Es por ello que consideramos que el documento debería advertir expresamente de estos peligros en los sistemas de IA que contemplen acciones de este tipo.

7. El documento tendría contemplar que las medidas de seguridad recomendadas deberían adoptar una perspectiva de "seguridad digital".

Este enfoque supone que el centro de análisis no debe estar en conceptos como "interés nacional", "seguridad nacional", "interés económico" o similares. Cuando hablamos de seguridad digital, nos referimos a la capacidad de los titulares de los datos de relacionarse con los sistemas de IA de manera beneficiosa para sus necesidades y evitando la exposición a riesgos para su autonomía e identidad.

8. El documento menciona el derecho a no ser objeto de decisiones individuales automatizadas sin intervención humana, de acuerdo con lo establecido en los Estándares de la RIPD (art. 29).

En ese sentido, creemos necesario que se haga referencia expresa a que dicha **intervención debe ser significativa, es decir, que tenga autoridad y competencia para cambiar la decisión.** De lo contrario, cualquier desarrollo de IA podría sortear este límite con solo insertar un acto humano aunque sea meramente testimonial.

9. Debería incorporarse expresamente el derecho a explicación en el catálogo de derechos de los titulares de los datos contemplados en el anexo.

El derecho a explicación constituye una garantía esencial para la protección del individuo en los sistemas de IA, ya que le permite contar con la información suficiente para ejercer las acciones o conductas que él crea conveniente. En este sentido, el derecho a la explicación implica que los responsables del tratamiento de datos deben cumplir un conjunto de acciones, como ser: explicar la lógica seguida por el sistema para la decisión, informar de la existencia y la forma de la intervención humana, entre otras.

10. Respecto al principio de licitud, se sugiere que la recomendación de revisar la normativa sobre protección de datos personales se extienda a la jurisprudencia aplicable y a instrumentos de *soft law* en materia de

derechos humanos (informes de relatores, guías, estándares, etc).

11. Respecto al **principio de lealtad**, se sugiere **incluir la condición económica, el género y las personas con discapacidad como otras categorías** sobre las cuales los modelos de IA no deben enfatizar información si conduce a un tratamiento discriminatorio arbitrario. Asimismo, se aconseja dejar una fórmula abierta para contemplar otras posibles categorías que merezcan una inclusión futura.

12. El documento establece adecuadamente que cuando surja una nueva finalidad para el tratamiento, debe haber una nueva solicitud de consentimiento. De todas maneras, consideramos que **debería recomendarse a los responsables que limiten al máximo posible la creación de nuevas finalidades posteriores a las previstas originalmente.**

13. El documento debería señalar la **prohibición de establecer sistemas de puntaje único para fines generales sobre las personas (*universal scoring*)**.

Los puntajes universales buscan reflejar una evaluación uniforme para las personas a través de múltiples acciones que estas realizan en su vida cotidiana. De este modo, se vuelven particularmente sensibles para la privacidad y la dignidad humana. Es por eso que estas iniciativas no deberían formar parte de ninguna acción de los gobiernos o de entidades privadas.

14. Sugerimos que se remarque la necesidad de que exista una **obligación de identificación** que permita que cada individuo conozca el sistema de IA en funcionamiento y la institución responsable del mismo. Debido a la asimetría de poder que suele existir, los sistemas de IA poseen una gran cantidad de información acerca del individuo, mientras este puede no conocer ni siquiera al operador del sistema. Es por eso que la identificación sería útil para disminuir la asimetría señalada.

Quedamos a disposición de la RIPD para seguir contribuyendo a la redacción del documento, sea a través de la clarificación de los puntos señalados o por medio de otras recomendaciones que forman parte del enfoque general que las organizaciones tienen sobre la implementación de estas tecnologías.

Referencias:

- "Universal Guidelines on Artificial Intelligence" (UGAI).

<https://thepublicvoice.org/ai-universal-guidelines/>

- Contribución del consorcio de organizaciones AISur a la consulta pública sobre "Ethics and Data Protection in Artificial Intelligence: continuing the debate" impulsada por el International Conference of Data Protection and Privacy Commissioners (ICDPPC).

<https://adc.org.ar/2019/05/09/etica-y-proteccion-de-datos-en-la-inteligencia-artificial/>

- "Una perspectiva de derechos para el Plan Nacional de Inteligencia Artificial", Asociación por los Derechos Civiles, disponible en:

<https://adc.org.ar/2019/07/18/una-perspectiva-de-derechos-para-el-plan-nacional-de-inteligencia-artificial/>

Firmantes:

Asociación por los Derechos Civiles (ADC) / Argentina

Cooperativa Autogestionaria Sulá Batsú / Costa Rica

Fundación Karisma / Colombia

Hiperderecho / Perú

R3D: Red en Defensa de los Derechos Digitales / México