

Algorithmic Decision Making

Rogelio Lizárraga Escobar A01742161

Introducción

La toma de decisiones algorítmica implica el uso de métodos computacionales que permiten a las máquinas completar tareas de manera automática, realizando decisiones que anteriormente hacían los humanos. Un ejemplo de esto es el seguro basado en el uso de Airbnb, el cual permite a los hosts asegurar propiedades dentro de un periodo de alquiler, en vez de pagar por una cobertura continua.

Riesgos Potenciales

La mercantilización de la información personal nos lleva a dudar si realmente estamos aplicando prácticas éticas, incluso legales, dentro del marco político aceptable y los principios de autodeterminación, pues limita la autodeterminación y sesga la toma de decisiones.

El Caso Práctico de Airbnb

El caso de Airbnb mencionado anteriormente es interesante porque el uso de algoritmos para determinar la solvencia de los prestatarios y establecer características basadas en el riesgo percibido puede producir sesgos. Estos sesgos podrían afectar negativamente a ciertos grupos de personas, perpetuando desigualdades preexistentes.

En el contexto de la toma de decisiones algorítmica, estos sesgos pueden surgir de varias maneras. Por ejemplo, los datos de entrenamiento utilizados para desarrollar el algoritmo pueden reflejar prejuicios históricos o sociales, lo que lleva a que el algoritmo reproduzca y amplifique esos mismos sesgos. Además, las decisiones algorítmicas pueden estar influenciadas por variables proxy que, aunque no son directamente discriminatorias, están correlacionadas con características protegidas, como la raza, el género o la situación socioeconómica. Esto puede resultar en la discriminación indirecta de ciertos grupos de usuarios. Por lo tanto, es importante examinar cómo estos algoritmos podrían contribuir a la discriminación o exclusión de ciertos usuarios y tomar medidas para mitigar estos riesgos.

Normativa Existente

Para asegurar un uso ético de las decisiones algorítmicas, es crucial que las organizaciones cumplan con las leyes y normativas locales. En nuestro país, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares regula el uso de datos personales, garantizando que estos no se utilicen de manera que viole los derechos de privacidad de los individuos. Además, leyes contra la discriminación aseguran que las decisiones no sean sesgadas en contra de ninguna persona basada en su raza, género, religión, o cualquier otra característica protegida.

En el marco internacional, se encuentran distintas normas, como las directrices del IEEE para sistemas autónomos y el marco de responsabilidad del NIST. Estas normas son esenciales para garantizar que los sistemas algorítmicos sean seguros, transparentes, y justos. Promueven el desarrollo de algoritmos que sean explicables y que cuenten con mecanismos de supervisión para detectar y corregir sesgos y errores.

Aplicación de la Normativa en un Contexto Similar al del Titanic

Si consideramos la normativa existente y la aplicamos a un caso similar al del Titanic, observamos que los datos utilizados no contienen información personal altamente sensible, lo que minimiza las preocupaciones de privacidad. Sin embargo, incluso en este tipo de casos, es fundamental que los algoritmos se desarrollen y utilicen de manera ética, garantizando la equidad y la transparencia en la toma de decisiones.

Conclusión

Es fundamental que las organizaciones sigan tanto leyes y normas locales como principios éticos globales, garantizando un enfoque transparente y responsable en todas las etapas del desarrollo y uso de algoritmos. Esto asegura que las decisiones algorítmicas cumplan con las regulaciones necesarias y respeten los principios éticos fundamentales, minimizando el riesgo de sesgo y discriminación.

Referencias

1. IEEE Standards Association. (2021). *IEEE 7000-2021: IEEE standard model process for addressing ethical concerns during system design*. Recuperado de <https://standards.ieee.org/standard/7000-2021.html>
2. National Institute of Standards and Technology (NIST). (2022). *AI risk management framework*. Recuperado de <https://www.nist.gov/itl/ai-risk-management-framework>
3. Cámara de Diputados del H. Congreso de la Unión. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Diario Oficial de la Federación. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010
4. Hardt, M., Price, E., & Srebro, N. (2016). Equality of opportunity in supervised learning. En *Advances in Neural Information Processing Systems (NeurIPS)*. Recuperado de <https://arxiv.org/abs/1610.02413>
5. O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.
6. Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.