Módulo 3 •

Agencia de datos y soberanía

Autora:
Javiera Atenas •

Traducido del inglés por Carolina Veiga •

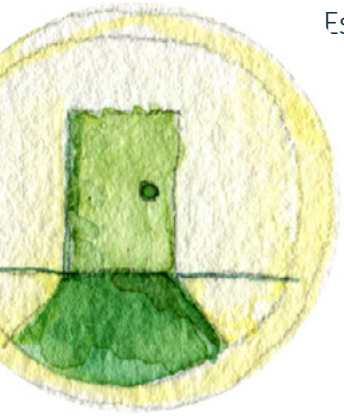
Este proyecto, Understanding data: praxis and politics está financiado por el EPSRC y Human Data Interaction Network+, con el número de concesión EP/R045178/1. **Caroline Kuhn H.**, es la investigadora principal y responsable del proyecto. •

Cómo citar este capítulo: Atenas, J. (2021). Agencia de datos y soberanía. En C. Kuhn, J. Atenas & L. Havemann (Eds.), Understanding Data: Praxis and politics. HDI - Data, Praxis and Politics. • https://doi.org/10.5281/zenodo.5137366. •

Módulo 3 • **Agencia de datos y soberanía** •

Contenido:

• Resumen y descripción de las unidades •



Este módulo tiene como objetivo presentar dos núcleos de elementos de datos, uno a nivel individual y otro a nivel colectivo. En la primera unidad, revisaremos el concepto, los principios y las habilidades necesarias para habilitar la agencia de datos personales y en la segunda unidad, exploraremos el concepto de soberanía de datos indígenas (SOB-DI).

En la primera unidad, revisaremos los conceptos y habilidades necesarios para habilitar la agencia de datos personales, entendida como la capacidad de los individuos para comprender y cuestionar los datos recopilados sobre ellos, para tomar decisiones informadas sobre sus datos al comprender el panorama legal de protección de datos y derechos de datos. Esto permitirá a las personas conservar y controlar sus datos (personales). Para hacer esto, necesitamos adquirir conocimiento de estos sistemas, poder identificarlos, pero también entender cómo funcionan.

En la segunda unidad, presentaremos los elementos y principios clave de la soberanía de datos indígenas (ID-SOV), un concepto relativamente reciente que puede entenderse como los derechos de los pueblos indígenas a poseer, controlar, acceder y poseer datos que deriven de sus necesidades y realidad social, fundamentada en los derechos a la autodeterminación y la gobernanza como se afirma en la Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas (DNUDPI).

• Objetivos de aprendizaje •

1. Comprender los elementos centrales de la agencia de datos personales

2. Entender cómo habilitar los derechos personales a través de la agencia de datos personales

3. Comprender los conceptos de agencia de datos y soberanía de datos

4. Adquirir habilidades para gestionar y cuestionar datos sensibles personales y colectivos

5. Comprender los principios básicos de la soberanía de datos autóctonos.

• Introducción multimedia • video-podcast •

Data Privacy and Consent | Fred Cate | TEDxIndianaUniversity
https://www.youtube.com/watch?v=2iPDpV8ojHA

Arizona State University School of Social Transformation Indigenous Data Sovereignty
https://www.youtube.com/watch?v=TXghvb6lPRI

• Glosario de términos y acrónimos • enlaces a Wikipedia cuando es posible •

Datos personales son cualquier información relacionada con una persona identificable. Datos personales

Agencia de datos es la capacidad del individuo para influir y dar forma a su trayectoria de vida según lo determinado por sus contextos culturales y sociales. La agencia en el ámbito digital permite a un individuo tomar decisiones informadas, donde sus propios términos y condiciones pueden ser conocidos y reconocidos a nivel algorítmico. Agencia de datos

Soberanía de los datos se refiere a que los datos deben estar sujetos a las leyes y estructuras de gobierno dentro de la nación en la que se recopilan. El concepto de soberanía de los datos está estrechamente relacionado con la seguridad de los datos, la computación en la nube y la **soberanía** tecnológica. Además, se puede

entender como la relación entre los datos y los grupos vulnerables o minoritarios, que deben tener agencia y voz sobre cómo se recopilan, comparten y retratan sus datos. Soberanía de los datos

Protección de datos es la relación entre la recopilación y difusión de datos, la tecnología, la expectativa pública de privacidad y las cuestiones legales y políticas que los rodean. También se conoce como privacidad de datos. Protección de datos

RGPD. El Reglamento general de protección de datos es un reglamento de la legislación de la UE sobre protección de datos y privacidad en la Unión Europea (UE) y el Espacio Económico Europeo (EEE). También aborda la transferencia de datos personales fuera de las áreas de la UE y el EEE. El objetivo principal del RGPD es dar control a las personas sobre sus datos personales y simplificar el entorno regulatorio para las empresas internacionales unificando la regulación dentro de la UE. RGPD

• Lecturas recomendadas •

1. Matthews, P. (2016). Data literacy conceptions, community capabilities. The Journal of Community Informatics, 12(3). https://openjournals.uwaterloo.ca/index.php/JoCI/article/view/3277/4300

2. Kennedy, H, Poell, T., & van Dijck, J. (2015). Data and agency. https://journals.sagepub.com/doi/pdf/10.1177/2053951715621569

3. Drummond, M. (2020). Independent IAM Organizations. IDPro Body of Knowledge, 1(1). https://bok.idpro.org/article/id/32/

4. Schwartz, P. M. (2003). Property, privacy, and personal data. Harv. L. Rev., 117. http://edshare.soton.ac.uk/15267/1/Schwartz-harvard-pdf.pdf

5. The GovLab: Selected Readings on Indigenous Data Sovereignty https://blog.thegovlab.org/post/selected-readings-on-indigenous-data-sovereignty

6. Kukutai & Taylor (Eds.). (2016). Indigenous Data Sovereignty: Toward an agenda. Acton ACT, Australia: ANU Press. http://www.jstor.org/stable/j.ctt1q1crgf

7. Lovett, R., Lee, V., Kukutai, T., Cormack, D., RAINIE, S. C., & Walker, J. (2019). Good data practices for Indigenous data sovereignty and governance. Good Data. Amsterdam: Institute of Network Cultures, 26-36. https://static1.squarespace.com/static/5b3043afb40b9d20411f3512/t/5b70e9c889858355258ae64a/1534126543958Good+data+practices+for+Indigenous+Data+Sovereignty+and+Governance+submitted.pdf

8. Rainie, S., Kukutai, T., Walter, M., Figueroa-Rodriguez, O., Walker, J., & Axelsson, P. (2019) Issues in Open Data - Indigenous Data Sovereignty. In T. Davies, S. Walker, M. Rubinstein, & F. Perini (Eds.), The State of Open Data: Histories and Horizons. Cape Town and Ottawa: African Minds and International Development Research Centre. Print version DOI: 10.5281/zenodo.2677801

• Recursos complementarios clave •

1. Herramienta en línea de la Unión Europea para la seguridad del procesamiento de datos personales https://www.enisa.europa.eu/risk-level-tool/

2. Agencia individual y datos personales IEEE https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e_personal_data.pdf

3. ICO ¿Qué son “controladores” y “procesadores”? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/

4. Gobernanza y soberanía de datos indígenas https://nni.arizona.edu/programs-projects/policy-analysis-research/indigenous-data-sovereignty-and-governance

5. Historia de la soberanía de datos indígenas https://www.gida-global.org/history-of-indigenous-data-sovereignty

3 • 1 • Agencia personal y datos •

Debido a que los flujos masivos de datos que circulan entre dispositivos, instituciones, industrias y usuarios marcan el comienzo de nuevas y preocupantes prácticas de vigilancia de datos, resulta vital reflexionar sobre si existen formas alternativas de Big Data, formas que permitan a los menos poderosos actuar con agencia frente al auge del poder de los datos.

Kennedy, Poell and van Dijck, 2015

• Introducción •

De acuerdo con la Iniciativa Global IEEE sobre Ética de Sistemas Autónomos e Inteligentes, los humanos no pueden responder de forma individual a cada algoritmo que rastrea su comportamiento sin herramientas tecnológicas respaldadas por políticas que les permitan hacerlo. Las personas pueden dar su consentimiento sin comprender completamente los términos y condiciones específicas de los acuerdos. Tampoco están preparados para comprender cómo el uso parcial de sus datos para informar algoritmos personalizados afecta sus elecciones a riesgo de erosionar su agencia. Aquí, tomamos la agencia como la capacidad de un individuo para influir y dar forma a su trayectoria de vida determinada por sus contextos culturales y sociales. La agencia en el ámbito digital permite a un individuo tomar decisiones informadas, donde sus propios términos y condiciones pueden ser reconocidos y respetados a nivel algorítmico.

Fomentar la agencia requiere de capacitar a que los menos poderosos, los vulnerables y las minorías tengan las habilidades que necesitan para desafiar las decisiones injustas y la dinámica de poder facilitada por los datos. Los estudiantes deben ser capaces de comprender cómo la recopilación, el procesamiento y el uso de datos da poder a algunos, pero no a otros. Esto crea un desequilibrio en la sociedad, ya que, según Atenas, Havemman y Timmermann (2020), puede marginar a quienes no pueden interactuar con los datos de manera efectiva.

3 • 1.1 • Entendiendo la agencia de datos personales •

> Para Kennedy, Poell and van Dijck (2015), reflexionar sobre la agencia es fundamental para pensar en la distribución del poder de los datos. Sin embargo, en el contexto de la datificación, las preguntas sobre la agencia se han visto eclipsadas por un enfoque en estrategias tecno-comerciales opresivas, como la minería de datos (p.2).

El IEEE recomienda que los gobiernos y las organizaciones ofrezcan mecanismos para fortalecer la agencia individual a través de políticas que permitan a las personas crear, curar y controlar los datos asociados con su identidad. Específicamente, recomiendan lo siguiente:

- **Crear:** proporcionar a cada individuo los medios para crear y proyectar sus propios términos y condiciones con respecto a sus datos personales que se puedan leer y acordar en un nivel legible por máquina.

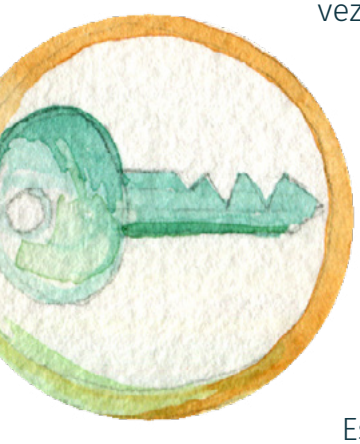
- **Curar:** proporcionar a cada individuo datos personales o un agente algorítmico, que pueden administrar para representar sus términos y condiciones en cualquier entorno real, digital o virtual.

- **Control:** Proporcione a cada individuo acceso a los servicios permitiéndoles crear una identidad confiable para controlar el intercambio seguro, específico y finito de sus datos.

Esto es importante, ya que las personas deben poder ver cómo los diferentes actores recopilan sus datos, que están creando perfiles que puede hacernos sujetos a todo tipo de usos de los malos usos de las decisiones automatizadas, lo que lleva a lo que se conoce como el problema principal-agente. Según la ciencia política y la economía (también conocida como dilema de agencia o problema de agencia), esto ocurre cuando una persona o entidad (el "agente") es capaz de tomar decisiones y / o tomar acciones en nombre de, o que impactan en otra persona o entidad.

Además, el IEEE sostiene que uno de los desafíos clave es definir cómo ciertos usos de los datos pueden afectar al individuo directamente.

Por ejemplo, la tarjeta de viaje de un usuario individual de subterráneo puede rastrear sus movimientos, por lo que debe protegerse de los usos que identifican o perfilan a esa persona para hacer inferencias sobre sus gustos o ubicación en general. Bajo los modelos comerciales actuales, es común que las personas den su consentimiento para compartir datos discretos, como datos de transacciones de tarjetas de crédito, respuestas a preguntas de prueba o cuántos pasos caminan. Una vez agregados, estos datos y los conocimientos asociados pueden llevar a conclusiones complejas y sensibles sobre las personas.



Los Principios de vinculación de la inteligencia artificial (LAIP) proponen el concepto de contestabilidad, que puede entenderse como cuando un sistema de IA impacta significativamente en una persona, comunidad, grupo o entorno, debe haber un proceso oportuno para permitir que las personas cuestionen el uso o salida del sistema de IA. Este principio tiene como objetivo garantizar la provisión de mecanismos eficientes y accesibles que permitan a las personas cuestionar el uso o la producción de un sistema de IA cuando impacta significativamente en una persona, comunidad, grupo o medio ambiente. La definición del umbral de "impacto significativo" dependerá del contexto, el impacto y la aplicación del sistema de IA en cuestión.

Saber que es posible reparar el daño cuando las cosas van mal es clave para garantizar la confianza pública en la IA. Se debe prestar especial atención a las personas o grupos vulnerables. Debe haber suficiente información sobre a qué información tienen los algoritmos y sus inferencias para que la contestabilidad sea efectiva. En el caso de decisiones que afecten significativamente los derechos, debe existir un sistema de supervisión eficaz, que haga un uso adecuado del juicio humano.

Por lo tanto, las Directrices de IA del Consejo Europeo proponen un marco para la agencia humana y la supervisión en el que los sistemas de IA deben apoyar la autonomía humana y la toma de decisiones, según lo prescrito por el principio de respeto por la autonomía humana. Esto requiere que los sistemas de IA actúen como facilitadores de una sociedad democrática, floreciente y equitativa apoyando la agencia del usuario y fomentando los derechos fundamentales, al tiempo que permiten la supervisión humana.

3 • 1.2 • Fomentando la agencia personal •

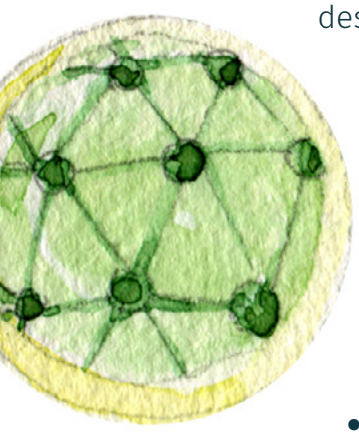
Para habilitar canales para el desarrollo de la agencia personal, necesitamos fomentar las discusiones para crear conciencia entre los estudiantes respecto del uso de (sus) datos. Se les debe alentar a considerar las estrategias que necesitan desarrollar para desafiar el uso de sus datos, ya que las personas deben poder tomar decisiones autónomas informadas con respecto a los sistemas de IA.

Se les debe dar el conocimiento y las herramientas para comprender e interactuar con los sistemas de IA en un grado satisfactorio y, cuando sea posible, estar capacitados para autoevaluar o desafiar el sistema de manera efectiva. Una buena forma de comenzar es discutir los derechos de las personas con respecto a la IA y luego preguntar si pueden desafiar las decisiones automatizadas. Además, debería discutirse cómo los diferentes países tienen diferentes enfoques para desafiar los algoritmos, y utilizando el contexto resultante del COVID-19, será beneficioso identificar cómo se utilizan y pueden impugnar esos datos.

En su artículo Por qué la agencia personal importa más que los datos personales, Searls (2018) afirma que "la primera razón por la que tenemos muy poca agencia en el mundo en red es que nos decidimos, allá por 1995, por un modelo para sitios web llamado cliente- servidor, que debería haber sido llamado vaca-ternero o amo-esclavo, porque siempre somos la parte más débil: dependiente, subordinada, secundaria. En términos regulatorios predeterminados, los clientes somos meros "sujetos de datos", y solo los operadores de servidores tienen el privilegio de ser "controladores de datos", "procesadores de datos" o ambos ", y" La segunda razón por la que la agencia importa más que los datos es que casi el todo el mercado actual de datos personales es adtech, y adtech es demasiado disfuncional, demasiado corrupto, sobrepasado con los datos que ya tiene, y absolutamente terrible llevando a cabo lo que fundamentó la recolección de esos datos, es decir, que las máquinas puedan adivinar lo que nosotros podríamos querer antes de que se disparen anuncios "relevantes" y "basados en intereses".

La privacidad en tanto derecho debe ejercerse; podemos definir la agencia como el

conjunto de habilidades necesarias para ejercer dicho derecho e incluye dos niveles de habilidades: una legal que significa ser capaz de comprender cómo se recopilan los datos, los términos y condiciones y las leyes que protegen a las personas, para desafiar la protección de datos; y una técnica, para comprender cómo las diferentes plataformas y dispositivos capturan datos y cómo prevenir y proteger los datos, esto incluye comprender cómo funcionan los datos encriptados que han sido pseudonimizados y que son reversibles.



Algunas de las habilidades para la agencia personal de datos que una persona necesita desarrollar, pueden resumirse como:

- La capacidad de comprender y dar consentimiento para uno o más propósitos específicos;

- Entender cuál y cómo el procesamiento de datos es necesario para celebrar un contrato;

- Comprender los procesos necesarios para cumplir con una obligación legal de proteger los intereses vitales del usuario o de otra persona;

- Comprender el proceso necesario para desarrollar una tarea en interés del público o según esté contenido en la autoridad oficial otorgada al controlador de datos;

- Comprender los intereses legítimos del responsable del tratamiento y los derechos y libertades del usuario, en particular los niños

3 • 1.3 • Agencia de datos y derechos personales •

Para poder tener agencia personal y ayudar a otros a convertirse en conocedores de los datos, es clave que las personas comprendan sus principales derechos sobre los datos, que según ICO, se pueden entender de la siguiente manera:

- **El derecho a ser informado** Se refiere a la conciencia de cómo las organizaciones deben proporcionar a los usuarios información sobre las actividades de tratamiento de datos que realizan normalmente a través de un aviso / política de privacidad. Los usuarios tienen derecho a que esta información se proporcione de manera concisa, transparente, inteligible, accesible, escrita en un lenguaje claro y sencillo (especialmente si está dirigida a un niño o un grupo vulnerable de usuarios), y debe proporcionarse de forma gratuita.

- **El derecho de acceso** Se refiere al derecho a acceder a nuestros propios datos personales y a comprender la información sobre cómo se están procesando sus datos. Por lo tanto, los usuarios deben comprender cómo solicitarlo y comprender la información que los controladores de datos les brindan.

- **El derecho a la rectificación** Se refiere a la capacidad de comprender el derecho a que se rectifiquen los datos personales si son parciales, inexactos o incompletos. Este derecho también implica que la rectificación debe comunicarse a los terceros destinatarios involucrados en el procesamiento de los datos, y también para comprender cómo impugnar las respuestas en los casos en que se rechace una solicitud.

- **El derecho a objetar** Se refiere a la capacidad de comprender y actuar sobre el derecho a oponerse a ciertas actividades de procesamiento en relación con los propios datos personales, lo que significa que cualquier persona puede oponerse al procesamiento de sus datos que incluyendo el interés público / ejercicio de la autoridad oficial, o para fines de investigación y estadísticas científicas / históricas.

• **El derecho de portabilidad de datos** Se refiere al derecho de las personas a obtener (en un formato legible por máquina) sus datos personales con el fin de transferirlos de un controlador a otro, sin que el procesador de datos se lo impida. Este derecho sólo se aplica a los datos personales y, como tal, no se aplica a los datos anónimos.

• **El derecho a supresión o eliminación** Se refiere al derecho a que se eliminen o eliminen los datos personales cuando los datos ya no sean relevantes para su propósito original, o el derecho a retirar el consentimiento o eliminar los datos personales si han sido procesados ilegalmente, solicitando que se borren sus datos y cese toda difusión. . Sin embargo, el derecho de supresión puede ser denegado en casos como cuando los datos personales se procesan con fines de archivo de interés público (por ejemplo, investigación científica) o cuando los datos son necesarios para la defensa legal o cuando los datos son necesarios para ejercer el derecho a la libertad de expresión o está siendo procesado con fines de salud de interés público.

• Actividad recomendada •

Para desafiar las decisiones automatizadas hacia la creación de una agencia personal, puede descargar u organizar un trabajo grupal en línea con sus estudiantes utilizando las actividades del derecho a contestar o impugnar, descargando las tarjetas.

El objetivo del derecho a contestar/impugnar es identificar los puntos ciegos de la IA que pueden generar consecuencias no deseadas, que surgen de nuestros prejuicios inconscientes o desigualdades estructurales arraigadas en la sociedad. El derecho a impugnar una decisión algorítmica puede revelar inexactitudes y otorgar agencia a las personas afectadas.

Después de terminar las actividades, se debe animar a sus estudiantes a compartir sus reflexiones con el resto de la clase.

3 • 2 • Soberanía de datos •

La naturaleza multifacética de la soberanía de los datos indígenas da lugar a una amplia gama de cuestiones, desde las dimensiones legales y éticas en torno al almacenamiento, la propiedad, el acceso y el consentimiento de los datos, hasta los derechos de propiedad intelectual y consideraciones prácticas sobre cómo se utilizan los datos en el contexto de la investigación, la política y la práctica

Kukutai and Taylor (2016)

3 • 2.1 • Entendiendo la soberanía de datos •

La soberanía de datos, según Kukutai & Taylor (2016) es "el derecho a mantener, controlar, proteger y desarrollar su patrimonio cultural, conocimientos tradicionales y expresiones culturales tradicionales, así como su derecho a mantener, controlar, proteger y desarrollar su propiedad intelectual sobre estos"

Este concepto de Soberanía de Datos Indígenas [ID-SOV] fue acuñado por En 2015 cuando académicos y líderes de las Primeras Naciones de Australia, Aotearoa / Nueva Zelanda, Canadá y los Estados Unidos definieron la soberanía de datos para establecer pautas para la publicación de datos indígenas (p. Ej., cultural, histórico, territorial), por lo tanto, las personas no indígenas deben obtener el consentimiento para la investigación antes de publicar cualquier dato sobre los pueblos indígenas.

Según IWGIA, la soberanía de los datos indígenas se define como el derecho de los pueblos indígenas a poseer, controlar, acceder y poseer datos que provengan de ellos y que se refieran a sus miembros, sistemas de conocimiento, costumbres o territorios. La soberanía de los datos indígenas se basa en los derechos inherentes a la autodeterminación y la gobernanza sobre sus pueblos, territorios y recursos, según lo estipulado en la Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas (DNUDPI), reconociendo así que los datos indígenas son un recurso estratégico por lo tanto, el concepto de soberanía de datos proporciona

un marco para el uso ético de la información indígena con el fin de avanzar en la autodeterminación de las comunidades indígenas, otorgándoles el derecho a ser tomadores de decisiones sobre cómo se utilizan sus datos.

El enfoque internacional para la protección de los datos personales y los derechos de privacidad es inadecuado para los pueblos indígenas, por lo que los países deben desarrollar e implementar leyes, regulaciones y estándares relacionados con la privacidad y los derechos de los pueblos indígenas a través de enfoques legales y regulatorios co-diseñados por ellos mismos basándose en los principios de ID-SOV.

ID-SOV puede verse como una fuerza impulsora para otorgar a las comunidades indígenas el derecho de autogobernanza de datos utilizando los valores, derechos e intereses de los pueblos indígenas para guiar la toma de decisiones sobre cómo se recopilan, consultan, almacenan y utilizan sus datos, dando a las comunidades control de sus datos a través de políticas y prácticas de gobernanza de datos y mediante mecanismos y marcos que reflejen los valores indígenas

3 • 2.2 • Principios de la gobernanza de los datos indígenas •

La Alianza Global de Datos Indígenas (GIDA) tiene como objetivo proporcionar una guía para el desarrollo conjunto de marcos y directrices para ID-SOV y difundir su implementación internacionalmente, a través de relaciones estratégicas con organismos y mecanismos globales. El Relator Especial de las Naciones Unidas sobre el derecho a la privacidad ha reconocido la importancia de ID-SOV para el Foro Permanente de las Naciones Unidas para las Cuestiones Indígenas y ha publicado algunas recomendaciones sobre Datos e Indicadores en el desglose de datos para la autodeterminación de los pueblos indígenas y con fines de desarrollo.

GIDA ha publicado una serie de principios para la gobernanza de los datos indígenas que incluye el derecho a crear valor a partir de datos indígenas de formas que se basan en las cosmovisiones indígenas y aprovechar las oportunidades dentro de la economía del conocimiento. Los cuatro principios pueden entenderse de la siguiente manera:

1. Beneficio colectivo: los entornos de datos deben diseñarse y funcionar de manera que permitan a los pueblos indígenas beneficiarse de los datos.

2. Autoridad de control: Se deben reconocer los derechos e intereses de los pueblos indígenas sobre sus datos y se debe empoderar su autoridad para controlar dichos datos.

3. Responsabilidad: Quienes trabajan con datos indígenas tienen la responsabilidad de dar a conocer cómo se utilizan esos datos para apoyar la autodeterminación y el beneficio colectivo de los pueblos indígenas. La rendición de cuentas requiere evidencia sustancial y abiertamente disponible de tales actividades y de los beneficios que pueden conferirse a los pueblos indígenas.

4. Ética: Los derechos y el bienestar de los pueblos indígenas deben ser la consideración principal en todas las fases del ciclo de vida de los datos y en todo el entorno de datos.

En Australia, el Colectivo de Soberanía de Datos Indígenas Maiam nayri Wingara y el Instituto Australiano de Gobernanza Indígena han desarrollado protocolos y principios para la Soberanía de Datos Indígenas y la Gobernanza de Datos Indígenas que implican que los pueblos indígenas tienen derecho a:

- Ejercer el control del ecosistema de datos, incluida la creación, el desarrollo, la administración, el análisis, la difusión y la infraestructura.
- Datos contextuales y desglosados (disponibles y accesibles a nivel individual, comunitario y de las Primeras Naciones).
- Datos que son relevantes y empoderan la autodeterminación sostenible y el autogobierno efectivo.

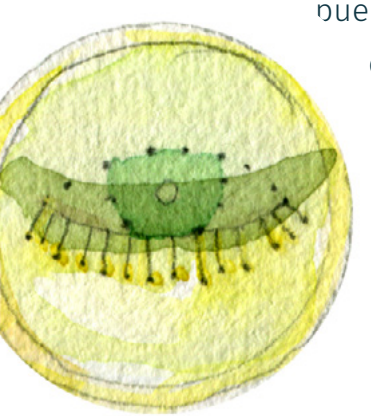
- Estructuras de datos que rinden cuentas a los pueblos indígenas y las Primeras Naciones.
- Datos que protegen y respetan sus intereses individuales y colectivos.

3 • 2.3 • Pueblos indígenas y datos abiertos •

Según Rainie, Kukutai, Walter, Figueroa-Rodríguez, Walker & Axelsson (2019) cuando los datos sobre pueblos indígenas se abren sin la participación e involucramiento de los pueblos indígenas, conduce a la invisibilidad y el sesgo, al mismo tiempo que brinda oportunidades para el desarrollo sostenible.

Por lo tanto, para ellos "la soberanía de datos indígenas (IDS) proporciona un marco para maximizar el beneficio de los datos abiertos para los pueblos indígenas y otros usuarios de datos indígenas y para afectar la administración de todos los datos", ya que "las naciones indígenas necesitan datos sobre sus ciudadanos, comunidades, tierras, recursos y cultura para tomar decisiones informadas. Sin embargo, pocas agencias de estadísticas oficiales, investigadores y recolectores de datos hacen una concesión significativa a los derechos indígenas en relación con los datos indígenas. A pesar de ser los titulares de los derechos en relación con los datos sobre ellos o para ellos, los pueblos indígenas de los Estados-nación siguen siendo periféricos a los canales de poder a través de los cuales se toman las decisiones consiguientes sobre las estadísticas indígenas ".

Para Walter, Lovett, Maher, Williamson, Prehn, Bodkin - Andrews & Lee (2020), los pueblos indígenas y las comunidades suelen estar representados en casos de desventaja social y los pueblos indígenas tienden a ser excluidos de las discusiones sobre la recopilación de datos, la gobernanza y el uso de tales datos, sin reconocer la agencia de datos, la cultura, los derechos y las necesidades de datos indígenas, silenciar sus voces durante la recopilación de datos procesados, marginando sus puntos de vista sociales, culturales y políticos a través de enfoques neocolonialistas, ya que a menudo existe una apropiación indebida de los datos en detrimento de los pueblos indígenas. Las voces indígenas deben incluirse



en las discusiones de múlti-actor en el sector de datos abiertos, y para que esto sea posible será clave desarrollar programas de creación de capacidades que sean culturalmente sensibles para ayudar a las comunidades indígenas a comprender cómo se recopilan los datos y cómo pueden ejercer sus derechos.

• Actividad recomendada •

Para comprender cómo se representa a los pueblos indígenas en los datos, pida a sus estudiantes que busquen datos sobre las comunidades indígenas y que utilicen la Lista de verificación de evaluación de sesgos (página 4) y que escriban un resumen de sus hallazgos y anímelos a compartir sus reflexiones con el resto del grupo.

Regreso a Entendiendo Data: Praxis + Politics