8_Ética_IA

July 13, 2025

Creado por:

Isabel Maniega

1 Consideraciones éticas en la recopilación de datos

Las consideraciones éticas son fundamentales en la recopilación de datos para garantizar la privacidad, la equidad y la transparencia. Abordar estas cuestiones no solo es responsable, sino también crucial para generar confianza con las partes interesadas.

1.0.1 Consentimiento informado

Obtener el consentimiento informado de los participantes es un imperativo ético. La transparencia es fundamental y los participantes deben comprender plenamente el propósito de la recopilación de datos, cómo se utilizarán sus datos y los posibles riesgos o beneficios involucrados. El consentimiento debe ser voluntario y los participantes deben tener la opción de retirar su consentimiento en cualquier momento sin consecuencias.

Los formularios de consentimiento deben ser claros y comprensibles, evitando un lenguaje excesivamente complejo o jerga legal. Se debe tener especial cuidado al recopilar datos sensibles o personales para garantizar que se respeten los derechos de privacidad.

1.0.2 Protección de la privacidad

Proteger la privacidad de las personas es esencial para mantener la confianza y cumplir con las regulaciones de protección de datos. Se debe utilizar la anonimización o seudonimización de datos para evitar la identificación de las personas, especialmente al compartir o publicar datos. Se deben implementar métodos de cifrado de datos para proteger los datos tanto en tránsito como en reposo, y resguardarlos del acceso no autorizado.

Se deben implementar controles de acceso estrictos para restringir el acceso a los datos solo al personal autorizado, y se deben establecer y respetar políticas claras de retención de datos, evitando el almacenamiento innecesario de datos. Se deben realizar auditorías de privacidad periódicas para identificar y abordar posibles vulnerabilidades o problemas de cumplimiento.

1.0.3 Sesgo y equidad en la recopilación de datos

Abordar el sesgo y garantizar la equidad en la recopilación de datos es fundamental para evitar la perpetuación de las desigualdades. Los métodos de recopilación de datos deben diseñarse para minimizar los sesgos potenciales, como el sesgo de selección o el sesgo de respuesta. Se deben

realizar esfuerzos para lograr muestras diversas y representativas, asegurando que los datos reflejen con precisión la población de interés. Es esencial brindar un trato justo a todos los participantes y fuentes de datos, y evitar estrictamente la discriminación basada en características como la raza, el género o el nivel socioeconómico.

Si se utilizan algoritmos en la recopilación o el análisis de datos, se deben evaluar y mitigar los sesgos que puedan surgir de los procesos automatizados. Se pueden considerar revisiones éticas o consultas con expertos cuando se trabaja con datos sensibles o potencialmente sesgados. Al adherirse a principios éticos durante todo el proceso de recopilación de datos, se protegen los derechos de las personas y se establece una base para la toma de decisiones responsable y confiable basada en datos.

1.0.4 Sesgo y representación

Garantizar que los métodos de recopilación de datos estén libres de sesgos y representen con precisión a poblaciones diversas es un desafío. Por ejemplo, las tecnologías de reconocimiento facial han enfrentado críticas por sesgo racial, donde ciertos grupos demográficos no son reconocidos con precisión, lo que genera preocupaciones éticas sobre la justicia y la igualdad.

1.0.5 Transparencia y rendición de cuentas

Mantener la transparencia en la forma en que se recopilan, utilizan y comparten los datos es un desafío, pero esencial para el cumplimiento ético. El desafío radica en comunicar prácticas de datos complejas de una manera comprensible para los usuarios. La falta de transparencia puede conducir a situaciones como el caso de Google Street View, donde Google fue criticado por recopilar más datos de los que reveló, incluidos detalles de la red Wi-Fi personal.

1.0.6 Cumplimiento legal y normativo

Navegar por el complejo panorama de las leyes internacionales de protección de datos, como el RGPD en Europa y las diferentes leyes en los distintos países, es un desafío importante para las organizaciones globales. El cumplimiento requiere una vigilancia constante y la adaptación a las normas legales en evolución.

1.0.7 Resumen: Ética de datos

Principios básicos de la ética de datos

- **Privacidad:** Proteger el derecho de las personas a controlar su información personal y garantizar que la recopilación de datos sea transparente y consensuada.
- **Seguridad:** Implementar medidas sólidas para proteger los datos de accesos no autorizados, infracciones y robos.
- **Justicia:** Garantizar que los datos se utilicen de manera justa y que no discriminen a ninguna persona o grupo.
- **Transparencia:** Hacer que los procesos de recopilación, análisis y uso de datos sean abiertos y comprensibles para todas las partes interesadas.
- **Responsabilidad:** Hacer que las organizaciones y las personas sean responsables de cómo recopilan, usan y comparten los datos.

Desafíos de la ética de datos

- **Equilibrar la innovación con la privacidad:** Encontrar el equilibrio adecuado entre aprovechar los datos para la innovación y respetar la privacidad de las personas puede ser un desafío.
- **Sesgo y discriminación:** Los datos y algoritmos pueden perpetuar sesgos inadvertidamente, lo que lleva a la discriminación si no se gestionan con cuidado.
- **Propiedad y control de los datos:** A medida que los datos se convierten en un activo valioso, determinar quién es su propietario y quién puede controlar su uso es cada vez más polémico.
- **Cumplimiento normativo:** Navegar por el complejo panorama de leyes y regulaciones de protección de datos en diferentes jurisdicciones se suma al desafío.

1.1 ¿Por qué es importante la recopilación precisa de datos?

La recopilación precisa de datos es crucial para garantizar la validez y confiabilidad de los hallazgos de la investigación. Apoya la toma de decisiones informada, mejora la precisión y exactitud, asegura la calidad y mantiene la integridad de la investigación. Sin datos precisos, las conclusiones extraídas de la investigación pueden ser erróneas o engañosas.

- **Toma de decisiones informada:** Los datos precisos proporcionan una base sólida para tomar decisiones que tienen más probabilidades de ser efectivas y beneficiosas. Ayudan a las partes interesadas a comprender el contexto y las implicaciones de sus elecciones.
- **Precisión y exactitud:** Los datos de alta calidad garantizan que los resultados de la investigación sean precisos y exactos, lo que genera confianza en los hallazgos y respalda la credibilidad de la investigación.
- **Garantía de calidad:** Garantizar la exactitud de los datos es esencial para mantener la calidad de la investigación. Ayuda a identificar y corregir errores, lo que conduce a resultados más confiables y válidos.
- **Integridad de la investigación** La recopilación precisa de datos mantiene la integridad del proceso de investigación. Garantiza que los hallazgos sean confiables y puedan ser replicados por otros investigadores.

1.2 El derecho a permanecer anónimo

Gracias a la legislación sobre privacidad de datos, encabezada por el RGPD de Europa y la CPRA de California, el consumidor ha obtenido voz y, con ella, el derecho a permanecer anónimo. De modo que, cuando una organización utilice mis datos (como inevitablemente hará), nunca podrán rastrearme hasta mí. Esta es la esencia de la anonimización de datos. La anonimización de datos es una categoría general que incluye el enmascaramiento de datos, la seudonimización, la agregación de datos, la aleatorización de datos, la generalización de datos y el intercambio de datos. Esta guía profundiza en cada una de estas técnicas de anonimización de datos y, a continuación, analiza los pros y los contras del proceso de anonimización, los desafíos que enfrenta y las direcciones para futuras investigaciones. Concluye revelando un enfoque innovador para garantizar la privacidad personal, el cumplimiento de las regulaciones, la confianza del cliente y el derecho a permanecer anónimo.

1.2.1 ¿Qué es la anonimización de datos?

La anonimización de datos es el proceso de ocultar o eliminar información de identificación personal (PII) de un conjunto de datos para proteger la privacidad de las personas asociadas con esos datos.

La anonimización de los datos hace que sea imposible reconocer a las personas a partir de sus datos, al tiempo que mantiene la información funcional para pruebas de software, análisis de datos u otros fines legítimos. La anonimización de datos transforma la PII y los datos confidenciales de tal manera que no se puedan vincular fácilmente a una persona específica. En otras palabras, reduce el riesgo de reidentificación, con el fin de cumplir con las leyes de privacidad de datos y aumentar la seguridad. El proceso de anonimización generalmente implica el enmascaramiento de datos PII, como nombres, direcciones, números de teléfono, detalles del pasaporte o números de la seguridad social. Con este fin, los valores se reemplazan o eliminan, mediante el uso de técnicas criptográficas, o agregando ruido aleatorio, para proteger los datos. Los datos anonimizados no pueden garantizar un anonimato completo, con la amenaza de reidentificación, en particular cuando los datos anonimizados se combinan con fuentes disponibles públicamente. Por lo tanto, los equipos de datos deben considerar cuidadosamente los riesgos y las limitaciones de sus herramientas y procesos de anonimización de datos cuando trabajan con datos personales o confidenciales.

1.2.2 El papel que desempeña la anonimización de datos en la protección de la privacidad personal

La anonimización de datos desempeña un papel fundamental en la protección de la privacidad personal al evitar la exposición y la explotación de la información confidencial de las personas. Con la cantidad cada vez mayor de datos que se recopilan y almacenan, el riesgo de que se pueda acceder a la información personal y hacer un uso indebido de ella (sin el conocimiento o el consentimiento de alguien) es mayor que nunca. Cuando se viola la información personal, no solo se trata de una violación de la seguridad para la organización, sino, lo que es más importante, de una violación de la confianza para el cliente o consumidor. Estos ataques pueden dar lugar a amplias violaciones de la privacidad, como incumplimiento de contrato, discriminación y robo de identidad. Al ocultar o eliminar la información de identificación personal de los conjuntos de datos, la anonimización de datos limita gravemente la capacidad de los usuarios no autorizados de acceder o utilizar la información personal. Además de prevenir violaciones de la privacidad y proteger los derechos de las personas, la anonimización de datos permite a las organizaciones cumplir con las regulaciones de privacidad de datos (como APPI, CPRA, DCIA, GDPR, HIPAA, PDP, SOX y más) que requieren que las empresas tomen medidas preventivas para proteger los datos confidenciales de las personas.

Igualmente importante es que, incluso después de que los datos se anonimicen, se pueden seguir utilizando para fines de análisis, información comercial, toma de decisiones e investigación, sin revelar nunca la información personal de nadie.

1.2.3 Tipos de anonimización de datos

Existen 6 tipos básicos de anonimización de datos, entre ellos:

1. **Enmascaramiento de datos:** El software de enmascaramiento de datos reemplaza datos confidenciales, como números de tarjetas de crédito, números de licencia de conducir y números de la Seguridad Social, con caracteres, dígitos o símbolos sin sentido, o datos enmascarados aparentemente realistas, pero ficticios. El enmascaramiento de datos de prueba los hace disponibles para fines de desarrollo o prueba, sin comprometer la privacidad de la información original. El enmascaramiento de datos se puede aplicar a un campo específico o a conjuntos de datos completos, utilizando una variedad de técnicas como la sustitución de caracteres, la mezcla de datos y el truncamiento. Los datos se pueden enmascarar a pedido o según un cronograma. El conjunto de enmascaramiento de datos incluye la tokenización

de datos, que sustituye irreversiblemente los datos personales con marcadores de posición aleatorios, y la generación de datos sintéticos, cuando la cantidad de datos de producción es insuficiente.

2. **Seudonimización:** la seudonimización anonimiza los datos reemplazando cualquier información de identificación con un identificador seudónimo o pseudónimo. La información personal que se reemplaza comúnmente incluye nombres, direcciones y números de la Seguridad Social. Los datos seudonimizados reducen el riesgo de exposición o uso indebido de información personal identificable, al mismo tiempo que permiten que el conjunto de datos se use con fines legítimos. En la ecuación de seudonimización vs. anonimización, la primera es reversible (a diferencia de las soluciones de tokenización de datos) y, a menudo, se usa en combinación con otras tecnologías que mejoran la privacidad, como el enmascaramiento de datos vs. el cifrado.

3. **Agregación de datos:** la agregación de datos, que combina datos recopilados de muchas fuentes diferentes en una sola vista, se usa para obtener información para una mejor toma de decisiones o análisis de tendencias y patrones. Los datos se pueden agregar en diferentes niveles de granularidad, desde simples resúmenes hasta cálculos complejos, y se puede hacer en datos categóricos, datos numéricos y datos de texto. Los datos agregados se pueden presentar en diversas formas y se pueden utilizar para diversos fines, como análisis, informes y visualización. También se puede realizar con datos que se han seudonimizado o enmascarado para proteger aún más la privacidad individual.

4. **Generación aleatoria de datos:** La generación aleatoria de datos, que mezcla aleatoriamente los datos para ocultar información confidencial, se puede aplicar a un conjunto de datos completo o a campos o columnas específicos de una base de datos. La generación aleatoria de datos, que suele utilizarse junto con herramientas de enmascaramiento de datos o tokenización de datos, es ideal para ensayos clínicos, ya que garantiza que los sujetos no solo se elijan al azar, sino que también se asignen aleatoriamente a diferentes grupos de tratamiento. Al combinar diferentes tipos de anonimización de datos, se reduce el sesgo y se aumenta la validez de los resultados.

5. **Generalización de datos:** La generalización de datos, que reemplaza valores de datos específicos por valores más generalizados, se utiliza para ocultar información de identificación personal (PII), como direcciones o edades, a terceros no autorizados. Sustituye categorías, rangos o áreas geográficas por valores específicos. Por ejemplo, una dirección específica, como 1705 Fifth Avenue, se puede generalizar al centro, al centro de la ciudad o a la zona alta de la ciudad. De manera similar, la edad de 55 años se puede generalizar a un grupo de edad llamado de 50 a 60 años, o adultos de mediana edad.

6. **Intercambio de datos:** El intercambio de datos reemplaza los valores de datos reales por otros ficticios, pero similares. Por ejemplo, un nombre real, como Don Johnson, se puede intercambiar por uno ficticio, como Robbie Simons. O una dirección real, como 186 South Street, se puede intercambiar por una ficticia, como 15 Parkside Lane. El intercambio de datos es similar al generador de datos aleatorios, pero en lugar de mezclar los datos, reemplaza los valores originales por otros nuevos y ficticios.

1.2.4 Técnicas de anonimización de datos

Existen 5 técnicas clave de anonimización de datos, entre ellas:

1. **Anonimato K:** El anonimato K garantiza que la información de ninguna persona pueda

distinguirse de al menos "K-1" otras personas en el mismo conjunto de datos. En otras palabras, para cualquier registro dado, hay al menos K otros registros en el conjunto de datos con valores idénticos para todos los atributos de identificación. Por ejemplo, si un conjunto de datos contiene información personal como nombres, direcciones y números de seguro social, y K se establece en 3, entonces la información de ninguna persona puede distinguirse de al menos otras 2 en el conjunto de datos. Esto significa que los piratas informáticos no podrán identificar a una persona específica dentro del conjunto de datos simplemente mirando los valores de los atributos de identificación, porque hay al menos otras 2 personas en el conjunto de datos con exactamente los mismos valores. El anonimato K nunca puede garantizar una protección de la privacidad del 100%, porque a medida que aumenta el valor de K, el riesgo de reidentificación disminuye, pero nunca se elimina por completo. Además, esta técnica de anonimización de datos no tiene en cuenta ningún factor externo a la hora de identificar a alguien, por lo que incluso cuando un conjunto de datos es K-anónimo, puede combinarse con otras fuentes de datos para volver a identificar a una persona específica.

2. **L Diversity**, que garantiza que la información de ninguna persona pueda distinguirse de al menos L otras personas del conjunto de datos en función de un atributo sensible, es una extensión de K Anonymity. Pero mientras que K Anonymity garantiza que la información de ninguna persona pueda distinguirse de al menos K-1 otras personas del conjunto de datos, L Diversity protege los atributos sensibles, así como los generales. Por ejemplo, si un conjunto de datos contiene atributos sensibles como una condición médica o medicamentos recetados, debe haber al menos L personas en ese conjunto de datos para cualquier valor específico del atributo sensible, a fin de no identificar a una persona específica. Al igual que K Anonymity, L Diversity no garantiza una protección total de la privacidad, por las mismas razones citadas en la sección anterior. Y la diversidad L es más difícil de implementar que el anonimato K, porque no solo tiene que identificar y proteger atributos sensibles, sino que solo puede funcionar cuando al menos L valores distintos para cada uno de esos atributos están presentes en el conjunto de datos.

3. **T Closeness:** T Closeness contribuye a la eficacia de la combinación de anonimato K / diversidad L al asegurar que la distribución de los atributos sensibles en el conjunto de datos coincida con la de la población objetivo, lo más fielmente posible. Por ejemplo, si un conjunto de datos determinado contiene no solo información personal identificable, sino también atributos sensibles como el ingreso, T Closeness garantiza que la distribución del ingreso en el conjunto de datos sea muy cercana a la de la población objetivo. De esa manera, el valor del ingreso no revela ninguna información sobre una persona en particular. Al igual que el anonimato K y la diversidad L, T Closeness no puede garantizar una protección completa de la privacidad, por las mismas razones citadas anteriormente. Y la cercanía T es incluso más difícil de implementar que el anonimato K o la diversidad L, porque no solo tiene que identificar y proteger atributos sensibles, sino que solo puede ser efectiva cuando la distribución de los atributos sensibles en el conjunto de datos es similar a la de la población.

4. **Privacidad diferencial:** La privacidad diferencial, que añade ruido aleatorio a los datos para que no sean identificables, es un marco matemático utilizado en el análisis, la elaboración de informes y la visualización de datos que busca equilibrar el riesgo de privacidad de un conjunto de datos determinado frente a su utilidad. Utiliza varias técnicas de aleatorización, como la perturbación y el muestreo. Un parámetro de nivel de protección de la privacidad, conocido como épsilon ( ), controla la cantidad de ruido añadido a los datos. Cuanto menor sea el valor de épsilon, mayor será el nivel de ruido necesario. La privacidad diferencial puede hacer que

los datos sean menos precisos, por lo que es importante encontrar el equilibrio adecuado entre la protección de la privacidad y la utilidad. Y como siempre hay una pequeña probabilidad de reidentificación (controlada por el parámetro de privacidad), no puede garantizar una protección completa.

5. **Respuesta aleatoria:** La respuesta aleatoria es una técnica de encuesta que funciona al decidir aleatoriamente si una pregunta se responde con sinceridad o si se da una respuesta predeterminada de Sí o No. Permite a las personas responder con sinceridad a preguntas delicadas, sin revelar sus respuestas reales. Esto se logra introduciendo un nivel de aleatoriedad en el proceso de encuesta, con el fin de evitar que los administradores de la encuesta conozcan la respuesta verdadera. En una encuesta sobre el consumo de drogas, por ejemplo, una de las preguntas podría ser "¿Alguna vez ha consumido drogas ilegales?". Esta técnica asigna aleatoriamente a cada encuestado la opción de responder honestamente o dar una respuesta predeterminada de "Sí" con una cierta probabilidad (digamos 0,5). La técnica de respuesta aleatoria se puede combinar con otros métodos de encuesta, como encuestas anónimas y encuestas autoadministradas, para proteger aún más la privacidad de los encuestados. Como concepto probabilístico, la respuesta aleatoria no puede brindar una protección integral de la privacidad, porque la reidentificación es posible, aunque sea de forma remota.

1.2.5 Anonimización de datos:

A continuación, se incluye un resumen de las ventajas y desventajas de la anonimización de datos:

Pros	Contras
Hace que la identificación de una persona en un conjunto de datos sea imposible o muy improbable	Puede reducir la utilidad de los datos al modificar o eliminar elementos PII importantes
Permite compartir datos con fines legítimos, como análisis e investigación	Puede permitir la reidentificación, si un atacante puede hacer referencias cruzadas de datos adicionales
Permite un cumplimiento más rápido y sencillo de las leyes de privacidad de datos	Puede requerir experiencia y herramientas especializadas, lo que aumenta la complejidad y el costo
Impide que los atacantes obtengan acceso a información confidencial	Puede no proporcionar protección total de la privacidad de los datos (si la reidentificación tiene éxito)
Minimiza el riesgo de errores, como la vinculación incorrecta de datos	Puede no funcionar con datos muy confidenciales o que tienen propiedades únicas
Reduce los costos, con la reutilización de datos sin consentimiento y sin necesidad de almacenamiento seguro	Puede consumir mucho tiempo y recursos y no es muy escalable

Creado por:

Isabel Maniega