Tecnológico de Monterrey

Campus Querétaro

Privacidad y Seguridad de los Datos

Uri Jared Gopar Morales A01709413

Inteligencia artificial avanzada para la ciencia de datos II
Grupo 501

Anonimización de los datos

Para poder anonimizar los datos en nuestro procesos de clasificación de imágenes, utilizamos un script el cual cortaba la imagen en original en 3 secciones dando de esta manera una vista más clara de nuestro objetivo principal, el cual era saber si existía en la cama una vaca parada, acostada o no habia vaca en la cama. Aunque al principio este proceso únicamente lo usamos para clasificar nos percatamos que también fue una solución al término del anonimato, debido a que podíamos observar de una mejor manera todos los objetos que contenía dicha foto. De esta manera fuimos capaces de ver que no existían datos sensibles los cuales pudieran poner en riesgo la identidad de nuestro socio formador o al CAETEC. Cabe aclarar que aunque no trabajemos con datos sensibles el socio formador nos pidió que no compartiéramos este dataset con ninguna persona que sea externa al proyecto.

Normativas

México:

Por el sector privado contamos **La Ley Federal de Protección de Datos Personales** en Posesión de los Particulares (LFPDPPP) fue instaurada en México el 5 de julio de 2010 con el objetivo de regular el manejo de datos personales en poder de las empresas. Le siguió de cerca el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2011 y los Lineamientos de Aviso de Privacidad en 2013.

Los negocios o servicios son obligados a brindar un manejo adecuado de los datos personales de sus clientes prospectos, garantizando así sus derechos de privacidad.

En esta ley están incluidos ciertos elementos que deben cumplir las entidades para garantizar la protección de datos personales, tales como:

- Tener el consentimiento del titular de la información.
- Informar para qué serán usados los datos de los clientes.
- Garantizar sus derechos ARCO (aceptación, rectificación, cancelación y oposición).

4 derechos de privacidad contenidos en la Ley Federal de Protección de Datos Personales
Acceso: se refiere al derecho que tienen los titulares de la información a recibir detalles del uso y gestión de sus datos personales.

- Rectificación: cuando la información es inapropiada o incompleta, las personas tienen derecho de solicitar una rectificación.
- Cancelación: en caso de que los datos no se estén gestionando correctamente, los titulares poseen el derecho de pedir una anulación de los mismos.
- Oposición: si el titular de la información personal decide oponerse al procesamiento de los datos está en todo su derecho.

Para el sector público contamos con la ley de **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)**, sin embargo, esta ley la cumplen las empresas gubernamentales hacia la protección de datos de los ciudadanos por lo que no tiene impacto en nuestro proyecto.

Suiza:

La protección de datos en Suiza también está regulada por la Ley Federal de Protección de Datos (LPD), que contiene:

- Normas generales sobre protección de datos
- Normativa sobre el tratamiento de datos por parte de particulares, organizaciones y autoridades federales
- Las funciones y competencias del Comisionado Federal de Protección de Datos e Información, principal autoridad de control

De acuerdo con la Ley, el tratamiento de datos personales debe cumplir los siguientes principios generales:

- Principio de licitud – Los datos personales sólo pueden ser tratados de manera lícita
- Principio de proporcionalidad – El tratamiento de datos personales debe realizarse de buena fe y debe ser proporcionado
- Principio de adecuación – Los datos personales sólo pueden ser tratados para la finalidad indicada en el momento de su recogida, que resulte evidente de las circunstancias o que esté prevista por la ley.
- Principio de transparencia – La recogida de datos personales y la finalidad del tratamiento deben ser evidentes para el interesado
- El tratamiento de datos sensibles y de perfiles de identidad también está contemplado en la Ley y los encargados del tratamiento de los mismos deben obtener el consentimiento expreso de los interesados. Los datos sensibles y los perfiles de identidad pueden contener datos que permitan evaluar las características esenciales de la personalidad de una persona. La divulgación injustificada de dichos datos a terceros se considera una infracción de la protección de datos y está sujeta a multas

El interesado debe conocer

- Todos los datos disponibles relativos al interesado
- La finalidad del tratamiento
- Las categorías de datos personales que se procesan
- Otras partes implicadas en el tratamiento.
- Si la recopilación o el procesamiento de datos personales es ilegal, el interesado puede solicitar que se detenga el procesamiento de datos y que se destruyan los datos personales.

El responsable del tratamiento de datos deberá garantizar un nivel adecuado de protección de datos mediante la aplicación de medidas técnicas y organizativas de protección y garantizar la confidencialidad, disponibilidad e integridad de los datos.

Unión Europea:

El Reglamento General de Protección de Datos (RGPD) es la ley de privacidad y seguridad. Aunque fue redactado y aprobado por la Unión Europea (UE), impone obligaciones a las organizaciones en cualquier lugar, siempre que dirijan sus datos a personas de la UE o los recopilen. El reglamento entró en vigor el 25 de mayo de 2018.

Principios de protección de datos:

- Licitud, lealtad y transparencia : el procesamiento debe ser lícito, justo y transparente para el interesado.
- Limitación de la finalidad : Debe procesar los datos para los fines legítimos especificados explícitamente al interesado cuando los recopiló.
- Minimización de datos : debe recopilar y procesar solo la cantidad de datos que sea absolutamente necesaria para los fines especificados.
- Exactitud : Debe mantener los datos personales exactos y actualizados.
- Limitación de almacenamiento : solo puede almacenar datos de identificación personal durante el tiempo que sea necesario para el propósito especificado.
- Integridad y confidencialidad : el procesamiento debe realizarse de tal manera que se garantice la seguridad, integridad y confidencialidad adecuadas (por ejemplo, mediante el uso de cifrado).
- Responsabilidad : el controlador de datos es responsable de poder demostrar el cumplimiento del RGPD con todos estos principios.

Seguridad de datos
Debes manejar los datos de forma segura implementando “ medidas técnicas y organizativas apropiadas ”.

Las medidas técnicas pueden abarcar desde exigir a sus empleados que utilicen autenticación de dos factores en las cuentas donde se almacenan datos personales hasta contratar proveedores de la nube que utilicen cifrado de extremo a extremo .

Las medidas organizativas son cosas como capacitaciones del personal , agregar una política de privacidad de datos al manual del empleado o limitar el acceso a los datos personales sólo a aquellos empleados de su organización que los necesitan

Privacidad en el uso de Imágenes para Inteligencia Artificial

La Ley Federal que Regula la Inteligencia Artificial, un marco normativo que busca regular el uso y comercialización de la inteligencia artificial.

La ley propuesta tiene como propósito que la utilización de la inteligencia artificial sea usada de manera responsable y ética, además de que busca garantizar el respeto a los derechos humanos de consumidores y proteger los derechos de propiedad intelectual.

Ley para la Regulación Ética de la Inteligencia Artificial y la Robótica

Artículo 16. El respeto de la protección de datos personales, derechos humanos, propiedad industrial, propiedad intelectual, quedan amparados conforme a las leyes en la materia durante el cumplimiento de esta ley.

Artículo 17. El desarrollo, creación, investigación y uso de la Inteligencia Artificial y la Robótica en los Estados Unidos Mexicanos, se realizará con los principios fundamentales de apego a la ética, el respeto a los derechos humanos, la perspectiva de género, y sin discriminación alguna por origen étnico, raza, religión, condiciones sociales y económicas.

Artículo 18. Ninguna entidad pública o privada, dentro del territorio nacional, podrá hacer mal uso de la Inteligencia Artificial y la Robótica con fines de manipulación social, discriminación o violación al estado de derecho.

Buenas prácticas éticas para Inteligencia Artificial.

Minimización de datos

La minimización de datos es un aspecto fundamental para garantizar que un sistema de IA solo utilice datos relevantes, evitando que acceda y procese cualquier uso indebido de información personal no esencial.

Encriptación

Las empresas deberían procurar ofrecer al menos una forma de defensa de cifrado contra fuentes maliciosas que intenten robar información confidencial que está siendo procesada por sistemas de IA.

Políticas transparentes de uso de datos

Desarrollar documentación y políticas que establezcan claramente cómo las tecnologías de IA utilizan los datos personales.

Auditoría y monitorización de sistemas de IA

Realizar controles y balances periódicamente para detectar cualquier discrepancia debido a acciones no confiables de fuentes internas o externas y asegurarse de que este tipo de eventos no pasen desapercibidos.

Los LINKS para nuestra investigación grupal son los siguientes, el documento nombrado "**Privacidad y Seguridad de Datos**" es nuestro proceso en el cual describe paso a paso las actividades que realizamos como equipo para poder proteger y gestionar de la mejor manera los datos brindados por nuestro socio formador, dentro de este documento igual se encontrara el Link a nuestra **"Política de Datos y Regulaciones de Privacidad**", pero para evitar confusiones la adjuntare abajo.

LINKS:

- Privacidad y Seguridad de Datos: Proceso detallado de cómo se trabaja con el set de datos brindados por el socio formador.
- Política de Datos y Regulaciones de Privacidad: Política creada uniendo las investigaciones de los integrantes del equipo.
- Bitácora de Buenas prácticas

REFERENCIAS:

- *Data Privacy Rankings - Top 5 and Bottom 5 Countries - Privacy HQ*. (s. f.). https://privacyhq-com.translate.goog/news/world-data-privacy-rankings-countries/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=rq&_x_tr_hist=true

- *Guia de proteccion de datos personales*. (2012, 13 julio). www.scjn.gob.mx.

- *INICIATIVA QUE EXPIDE LA LEY PARA LA REGULACIÓN ÉTICA DE LA INTELIGENCIA ARTIFICIAL PARA LOS ESTADOS UNIDOS MEXICANOS, SUSCRITA POR EL DIPUTADO IGNACIO LOYOLA VERA Y LEGISLADORES INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PAN*. (2024, season-02). .gobernacion.gob.mx. http://sil.gobernacion.gob.mx/Archivos/Documentos/2023/04/asun_4543395_20230413_1680209417.pdf

- Ivana. (s. f.). *Privacy and data protection laws in Switzerland | Secure Swiss Data*. Secure Swiss Data - Encrypted Email Service And Secure Collaboration. https://secureswissdata-com.translate.goog/switzerland-privacy-data-protection-laws/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=rq
- *LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES*. (2010, 5 julio). www.diputados.gob.mx. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
- Ley Federal de Protección de Datos: ¿qué es y cuándo es aplicable? (2021, 13 octubre). *Docusign*. https://www.docusign.com/es-mx/blog/proteccion-de-datos-personales

- *Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I | Revista .Seguridad*. (s. f.). https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

- *Normativa y legislación en PDP – Marco Internacional de Competencias de Protección de Datos Personales para Estudiantes*. (s. f.). https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

- Wolford, B. (2023, 14 septiembre). *Recital 78 – Appropriate technical and organisational measures*. GDPR.eu. https://gdpr-eu.translate.goog/recital-78-appropriate-technical-and-organisational-measures/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=rq

- Wolford, B. (2024, 29 agosto). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr-eu.translate.goog/what-is-gdpr/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=rq