

[PAN] Nociones de Privacidad (Resumen)

¿Qué es la privacidad?

Depende de a qué definición recurramos puede ser:

- La capacidad de un individuo o un grupo de aislarse o aislar información sobre sí mismo.
- La privacidad evoluciona y se desarrolla a través de la percepción del individualismo que enfatiza el valor moral de lo individual
- La capacidad de individuos, grupos o instituciones para determinar ellos mismos cuando, como y hasta qué punto la información sobre ellos es comunicada a los demás.

¿Quienes son los adversarios?

Dependiendo del contexto son “Los Demás”, compañías o estados.

Privacidad y Seguridad

La seguridad es un medio para alcanzar la privacidad, la seguridad coincide con la privacidad en:

- La existencia de adversarios
- Muchos principios de diseño seguro también se aplican a la privacidad

Por otro lado la seguridad y la privacidad se diferencian en lo siguiente:

- La privacidad transciende el dominio digital
- Modelo: Actores débiles y en ocasiones, adversarios poderosos
- No se puede asumir la existencia de Terceras partes de confianza
- Susceptibilidad a la presión por parte de gobiernos, empleadores o presión social.

Ataques de Inferencia

Ataques de inferencia estadística en datos observados

Los datos observados pueden decírnos mucho más de lo esperado ya que el ser humano es predecible. Se puede observar una serie de datos de una base de datos para inferir información mediante el uso de un predictor estadístico. Por ejemplo, observando los likes que da una persona en facebook como base para la predicción se pueden obtener atributos que la gente considera privados. Por ejemplo, se pudo ver que la gente que daba like a cosas relacionadas con tormentas, el reporte Colbert y Ciencia tenía una inteligencia elevada, mientras que, por otro lado, la gente que daba like a cosas relacionadas con Sephora, Harley Davidson y Lady Antebellum tendían a tener baja inteligencia.

Desanonymización por enlaces de datos

Los datos anonimizados pueden ser desanonymizados enlazando atributos externos. Cuanto más escasos sean los datos, más únicos son y más fácil es enlazarlos. Un ejemplo de esto es el caso del concurso de minado de datos de Netflix, en el que con datos anonimizados, que consistían en el ID de un usuario, el ID de una película, la puntuación que le dio a esta y la fecha, se logró identificar una cifra elevada de usuarios cruzando los datos con los de IMDb comparando los usuarios que habían dado puntuaciones similares a películas más o menos en el mismo tiempo. Otro ejemplo de desanonymización por enlace es la que se basa en localización. Obteniendo trazas GPS de un área se puede desanonymizar a un usuario basándose en dónde pasa mucho tiempo y dónde pasa el día.

GDPR

Datos personales

Son cualquier información relacionada con un individuo que lo puede identificar de forma directa o indirecta. Nombres y direcciones de correo electrónico son datos personales obvios, otros datos como la localización, etnia, género, biometría, creencias religiosas, Cookies y opiniones políticas también pueden ser considerados datos personales. Los datos pseudoanónimos también caen bajo esta definición si es fácil relacionar a alguien con un ID.

Principios más importantes de la GDPR

- Minimización de datos: Se debe recolectar y procesar solo los datos que sean absolutamente necesarios para el propósito especificado
- Integridad y Confidencialidad: El procesado debe realizarse de tal forma que se asegure la seguridad, integridad y confidencialidad.

From:

<https://www.knoppia.net/> - Knoppia



Permanent link:

https://www.knoppia.net/doku.php?id=pan:res_nociones_privacidad

Last update: **2025/01/02 19:17**