mdt.

Ex Datis, Claritas

Qué es la privacidad diferencial

Qué es la privacidad diferencial, cómo funciona y por qué permite analizar y compartir datos de clientes con una garantía matemática de privacidad.

Manuel Delgado Tenorio · 17 de abril de 2019

Publicado originalmente en www.manueldelgado.com/blog/que-es-la-privacidad-diferencial



La privacidad diferencial es un conjunto de técnicas que permiten que recopilemos y compartamos datos con la "garantía matemática" de que las personas que proporcionaron esos datos no se van a ver afectadas en modo alguno.

En el terreno del **Customer Analytics**, la privacidad diferencial nos permite entrenar modelos con datos de clientes con la tranquilidad de que el modelo no va a aprender ni a recordar detalles de ningún cliente específico.

Podemos prometer a cada cliente que sus datos concretos no serán revelados, incluso aunque se combinen con otros conjuntos de datos. Esa promesa no es un simple compromiso de marketing o legal, sino que se basa en los fundamentos matemáticos sobre los que se sustenta la privacidad diferencial.

Cómo funciona la privacidad diferencial

Para proteger los datos sensibles de cada sujeto, cuando se lance una consulta a un sistema que incorpore la privacidad diferencial, este **modificará el resultado de la consulta añadiéndole nuevos datos (ruido) extraídos aleatoriamente de una distribución generada a partir de los datos originales.**

Así, un conjunto de datos que incorpore este concepto al que preguntemos algo como "*¿cuántos clientes que nos llamaron ayer tienen un saldo en cuenta superior a 100.000 euros?*" **no nos devolverá la cifra exacta y real,** sino un número cercano a ella resultante de sumarle un valor (positivo o negativo).

El objetivo que se persigue con la inclusión de esos datos aleatorios es, entre otros, que no se puedan combinar las respuestas de varias consultas para identificar los datos de alguien concreto.

La clave de este método está en cómo se calcula la intensidad del ruido que se añade a los resultados. **Mucho ruido resta utilidad a los datos.** Poco ruido, en cambio, permite estimar la realidad con relativo poco esfuerzo. En privacidad diferencial se manejan conceptos como la "**pérdida de privacidad**" o el "**presupuesto de privacidad**", que son variables sobre las que hay que tomar decisiones para ajustar los parámetros con los que se va a trabajar.

La manera en la que se determina esa distribución de la que se extraen los valores con los que se alteran los resultados es matemáticamente compleja. Yo no sería capaz de explicarla con más detalle sin meter la pata. Si tienes curiosidad, puedes leer papers como este de la investigadora que dio origen a esta técnica.

Por qué es necesaria la privacidad diferencial

La privacidad diferencial nació dentro del contexto de la publicación y compartición de datos con fines de investigación. Un problema habitual en ese ámbito es la reticencia a dar acceso a los datos con los que cuenta un equipo o institución, por miedo a que se pueda desvelar la identidad de quienes proporcionaron sus datos para el propósito original.

Existen otros enfoques para proteger la privacidad de los datos, pero no son tan eficaces. Algunos ejemplos:

- La **anonimización** de los datos produce pérdida de utilidad de esos mismos datos. Cuanto más anonimizados, menos información útil contienen. Si un dato mantiene un elevado nivel de utilidad, probablemente no está bien anonimizado.
- La **agregación** o resumen de los datos no impiden la identificación de personas en casos en los que se pueden correlacionar los datos agregados con otras fuentes de información complementarias.
- La publicación de datos aparentemente **inocuos** choca con múltiples problemas... empezando por la definición de "dato inocuo". Actividades comunes y ordinarias de nuestro día a día pueden permitir nuestra identificación. La creación de nuevos patrones de actividades supuestamente inocuas pueden revelar información relevante sobre nosotros (p.ej. - problemas de salud).
- La **restricción del tipo de consultas** que se pueden hacer sobre los datos suele chocar con limitaciones de utilidad (si limitas demasiado, vuelves inútil el sistema) y con limitaciones técnicas (p.ej. - cómo determinar al vuelo qué consultas son aceptables y cuáles no). Y, desde luego, no es aplicable cuando se publican los datos, sin más.

Actualmente, crece en magnitud y relevancia el debate acerca de la ética en el manejo y explotación de datos masivos. Debemos familiarizarnos con conceptos como este o el de inteligencia artificial explicable.

Aplicación en la empresa

Aunque surgiera alrededor de la investigación y los datos abiertos, **donde más interés hay ahora mismo por la privacidad diferencial es en el ámbito comercial.**

La explotación inteligente de los datos es, cada vez más, la base de muchos negocios, pero esa explotación choca directamente con los intereses y los (fundados) miedos de los consumidores. La privacidad diferencial propone una solución de compromiso en ese conflicto.

Bien aplicadas, estas técnicas facilitan determinadas operaciones que son claves hoy día:

- Recopilar hábitos de uso y todo tipo de eventos de forma ofreciendo un nivel de confianza notablemente superior al de cualquier otro enfoque
- Explotar esos datos dentro de la organización con libertad
- E incluso compartir los datos fuera de la organización sin riesgos reputacionales ni legales

Aunque Cynthia Dwork, autora del paper que he enlazado antes y pionera de la privacidad diferencial, trabaja en Microsoft, las dos empresas más conocidas hoy por la aplicación de este concepto son Google y Apple (los vínculos son a los papers donde explican en detalle cómo la aplican).

No se trata de un algoritmo, es una definición

Cuando hablamos de privacidad diferencial, **no hablamos de un algoritmo concreto ni, por supuesto, de una herramienta tecnológica.**

> *La privacidad diferencial es, ante todo, una definición, un acuerdo sobre un objetivo de privacidad y las condiciones matemáticas que se han de dar para estar en condiciones de lograrlo.*

La implementación concreta puede variar de un caso a otro y, a su vez, un mismo caso se puede resolver por medio de algoritmos distintos. Lo que es relevante es que todo ese sistema se mantenga dentro del marco de la definición de la privacidad diferencial.

Por tanto (y aquí quería llegar yo), la privacidad diferencial no es algo que se pueda "comprar" fácilmente. No es una pieza de software concreta, sino que es una forma de trabajar, un *mindset* que debe abarcar todo el sistema.

Es cierto que comienza a haber librerías que paquetizan el concepto que nos ocupa para casos de uso concretos, en stacks tecnológicos específicos. Es el caso de la librería de TensorFlow que publicó Google hace poco.

Salvo que tu caso de uso se ajuste y se limite a algo que ya está previsto y paquetizado (**y esto es muy poco frecuente**), la implementación de la privacidad diferencial es algo que habrá que tener en cuenta en el diseño del sistema e incorporarlo de forma específica y personalizada. Además, y esto es muy importante, el concepto ha de abarcar la totalidad del sistema.

Dicho de otro modo: que tus Data Scientists usen, por ejemplo, la librería de TensorFlow que menciono más arriba para entrenar algunos modelos no convierte, por arte de magia, todas tus prácticas de análisis de datos en respetuosas con el concepto de privacidad diferencial.

¿Qué hay más allá?

En este artículo, he querido resumir lo que he aprendido sobre este concepto en las últimas semanas.

He escrito **otro artículo sobre los dos tipos de privacidad diferencial** (local y global) y las **críticas** que se le hacen tanto al concepto genérico como a varias de sus implementaciones.

PARA SEGUIR LEYENDO
La otra gran técnica para compartir datos sin exponer a nadie son los datos sintéticos. Todo lo que he escrito sobre el tema, en privacidad y datos sintéticos.



Sobre el autor
Manuel Delgado Tenorio
Manuel Delgado Tenorio es asesor independiente de estrategia de datos e inteligencia artificial, profesor e investigador. Cofundó y vendió una *startup* de inteligencia artificial, fue socio de la práctica de Data & Analytics para servicios financieros en EY y responsable de Data Analytics para el sur de Europa en AWS. Es profesor asociado en IE University, donde imparte la primera asignatura de grado sobre Customer Lifetime Value en España, investiga sobre el CLV en su doctorado en la Universidad Complutense de Madrid y es autor del libro "Customer Lifetime Value (CLV): No todos tus clientes valen lo mismo".

manueldelgado.com · **LinkedIn** · **X**

Recibe cada artículo en tu correo con la newsletter Ex Datis, Claritas: manueldelgado.com/newsletter/suscribete