Privacidad desde el Diseño Jurisprudencia y Casos Emblemáticos

Trabajo Académico

Asignatura: Privacidad y Anonimidad

Máster en Ciberseguridad

Autor: [Tu Nombre]

Fecha: 13 de diciembre de 2025

Índice

1 Introducción

Cuando hablamos de *Privacidad desde el Diseño*, nos referimos a un cambio fundamental en cómo protegemos los datos personales. Ya no se trata solo de reaccionar ante problemas, sino de integrar la privacidad desde el primer momento en el desarrollo de cualquier sistema o tecnología. En este trabajo, vamos a analizar cuatro casos que han marcado un antes y un después en nuestra comprensión de la privacidad digital, demostrando por qué es tan importante incorporar estas protecciones desde el inicio.

Los casos que veremos abarcan tanto aspectos técnicos —como la reidentificación de datos o el cifrado— como cuestiones legales —como el derecho al olvido o la vigilancia masiva—, dándonos una visión completa de los desafíos actuales en protección de datos.

2 Snowden y vigilancia masiva (NSA, PRISM)

3 Casos de reidentificación de datos en EE.UU. y Europa

3.1 Caso Netflix (EE.UU., 2006-2008)

En 2006, Netflix lanzó un concurso público ofreciendo un millón de dólares a quien mejorara su algoritmo de recomendaciones. Para ayudar a los participantes, liberaron un conjunto de datos con más de 100 millones de calificaciones de películas de unos 500.000 usuarios, quitando antes información identificativa como nombres o correos electrónicos [1].

Pero aquí viene lo interesante: unos investigadores demostraron que esta anonimización no era tan segura como parecía. Cruzando los patrones de calificaciones y fechas con información pública de IMDb, lograron identificar a varios usuarios, exponiendo así todo su historial de visualización en Netflix. Lo que este caso nos enseña es que nuestros gustos en películas pueden ser tan únicos como una huella digital, incluso en medio de millones de registros.

3.2 Caso de datos de movilidad en Europa (2013)

Un equipo de investigadores europeos se puso a estudiar datos de telefonía móvil anonimizados [2]. Lo que descubrieron es bastante sorprendente: con solo **cuatro puntos espacio-temporales** (básicamente, saber dónde estuvo alguien y a qué hora en cuatro

momentos diferentes), podían identificar al 95 % de las personas en un conjunto de datos de 1.5 millones.

Esto es importante porque hoy en día nuestras operadoras de telefonía y muchas aplicaciones recogen constantemente estos datos de ubicación. El estudio nos muestra claramente que simplemente agregar datos o quitar nombres no nos protege realmente cuando nuestros patrones de movimiento son tan personales.

3.3 Caso de datos médicos del NHS Reino Unido (2017)

El sistema de salud público británico (NHS) compartió datos de pacientes con Google DeepMind para proyectos de investigación médica. Aunque los datos estaban "pseudonimizados"(es decir, reemplazaron identificadores directos por códigos), unos investigadores encontraron puntos débiles importantes. Usando algoritmos de aprendizaje automático, demostraron que combinando solo tres datos comunes —código postal, fecha de nacimiento y género— ya se podía volver a identificar a personas en grandes bases de datos médicas.

Este ejemplo nos recuerda por qué el GDPR considera los datos de salud como especialmente sensibles, y nos hace ver que necesitamos técnicas de protección mucho más sólidas que la simple sustitución de identificadores.

3.4 Lecciones técnicas para la Privacidad desde el Diseño

De todos estos casos, podemos sacar algunas conclusiones clave:

1. **La anonimización no es algo absoluto:** No existe eso de "datos completamente anónimos", sino diferentes niveles de riesgo que tenemos que evaluar constantemente.

2. **Somos más únicos de lo que pensamos:** Casi cualquier conjunto de datos detallado contiene combinaciones de atributos que son específicas de cada persona.

3. **Las técnicas tradicionales tienen límites:** Métodos como la k-anonimidad, que aseguran que cada registro sea similar a otros varios, pueden fallar cuando alguien cruza los datos con información adicional.

4. **Necesitamos técnicas más avanzadas:** Enfoques como el *diferencial de privacidad*, que añade cierto ruido"matemático controlado a los datos, ofrecen garantías de privacidad mucho más sólidas [5].

4 Google Spain vs. AEPD (TJUE, derecho al olvido)

4.1 Antecedentes y contexto del caso

Todo empezó en 2010 cuando Mario Costeja González, un ciudadano español, buscó su nombre en Google y encontró algo incómodo: enlaces a dos anuncios de 1998 en el periódico La Vanguardia que hablaban sobre la subasta de sus bienes por deudas con la Seguridad Social [6].

Para Costeja González, esta información ya no tenía relevancia después de más de una década, así que pidió tanto a Google como al periódico que la eliminasen. Google se negó, lo que llevó a Costeja a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD). Cuando la AEPD le dio la razón, Google apeló y el caso terminó en el Tribunal de Justicia de la Unión Europea.

4.2 Cuestiones jurídicas fundamentales

El Tribunal de Justicia de la Unión Europea tuvo que abordar tres cuestiones fundamentales en este caso. En primer lugar, se planteó si la normativa europea de protección de datos podía aplicarse a un motor de búsqueda como Google, que aunque tiene su sede central fuera de la Unión Europea, cuenta con una filial operativa dentro de su territorio. En segundo término, el Tribunal debía determinar si la actividad de indexar, almacenar y mostrar resultados de búsqueda constituía un ńtratamientoż de datos personales que hiciera responsable a Google conforme a la ley. Por último, y quizás lo más relevante para los ciudadanos, el Tribunal tuvo que dilucidar si podemos ejercer un derecho a solicitar la eliminación de enlaces a información que nos afecta, incluso cuando esa información fue publicada originalmente de forma lícita por terceros, como podrían ser periódicos u otras fuentes.

4.3 La sentencia del TJUE (13 de mayo de 2014)

El Tribunal respondió que sí a las tres preguntas, estableciendo precedentes importantes:

4.3.1. Responsabilidad de los motores de búsqueda

El TJUE determinó que lo que hace un motor de búsqueda —recolectar, indexar, almacenar y mostrar información personal— sí cuenta como "tratamiento de datos". Esto significa que Google no era un simple intermediario técnico, sino responsable de lo que hacía con esos datos.

4.3.2. Nacimiento del derecho al olvido digital

La sentencia estableció que tenemos derecho a pedir a los motores de búsqueda que eliminen enlaces a información nuestra cuando:

- La información ya no es **adecuada** para los fines originales
- Ha perdido **relevancia** con el tiempo
- Resulta **excesiva** en relación con lo que se pretende
- No está actualizada o es **inexacta**

Pero este derecho no es absoluto. Hay que equilibrarlo caso por caso con otros derechos como la libertad de expresión o el interés público.

4.3.3. Aplicabilidad extraterritorial

El Tribunal confirmó que la ley europea se aplicaba a Google porque tenía una filial en España a través de la cual desarrollaba su actividad comercial.

4.4 Impacto y consecuencias

La sentencia del TJUE tuvo consecuencias muy prácticas e inmediatas. Tras conocerse el fallo, Google no tardó en poner en marcha un formulario específico para que los ciudadanos europeos pudieran solicitar la eliminación de enlaces a información personal. Si miramos las cifras, el impacto fue enorme: en apenas cinco años, la compañía recibió peticiones para borrar más de 3,5 millones de URLs, de las cuales aceptaron alrededor del 45 %. Esto nos muestra que el "derecho al olvido"no era una mera idea teórica, sino una demanda social real y palpable.

A nivel normativo, el camino que abrió este caso fue decisivo. El principio que estableció el Tribunal se materializó y amplió en el **Reglamento General de Protección de Datos (GDPR)** de 2018, donde quedó consagrado como el "derecho de supresión.[en] su artículo 17. El GDPR no solo recogió el testigo, sino que fue más allá, definiendo con mayor precisión las condiciones para ejercer este derecho y reforzando significativamente las obligaciones de todas las empresas y organizaciones que manejan nuestros datos personales.

Sin embargo, a pesar de estos avances, la sentencia dejó al descubierto y sin resolver una serie de tensiones fundamentales. El debate sigue vivo hoy entre el derecho a nuestra privacidad y el derecho colectivo a estar informados; entre la protección de datos personales y el interés público periodístico o histórico; y entre la soberanía normativa de Europa

y la naturaleza global y sin fronteras de Internet. Estos dilemas no tienen una respuesta fácil, y su resolución sigue siendo uno de los grandes retos del mundo digital en el que vivimos.

4.5 Implicaciones para la Privacidad desde el Diseño

Este caso nos deja varias enseñanzas importantes para el diseño de sistemas:

1. **Diseñar pensando en el olvido:** Los sistemas deberían incluir desde el principio mecanismos para eliminar datos personales cuando sea necesario.

2. **Evaluar el impacto:** Motores de búsqueda y plataformas similares deben evaluar cómo sus sistemas afectan a nuestros derechos de privacidad.

3. **Hacer los algoritmos más transparentes:** La sentencia resalta la necesidad de entender mejor cómo los algoritmos deciden qué información mostrarnos y en qué orden.

5 Apple vs. FBI (cifrado y puertas traseras)

Referencias Bibliográficas

Referencias

[1] Narayanan, A. y Shmatikov, V. (2008). *Robust de-anonymization of large sparse datasets*. En 2008 IEEE Symposium on Security and Privacy (pp. 111-125). DOI: 10.1109/SP.2008.33.

[2] de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. y Blondel, V. D. (2013). *Unique in the crowd: The privacy bounds of human mobility*. Scientific Reports, 3(1), 1376. DOI: 10.1038/srep01376.

[3] de Montjoye, Y.-A., Radaelli, L. y Singh, V. K. (2015). *Unique in the shopping mall: On the reidentifiability of credit card metadata*. En 2015 IEEE European Symposium on Security and Privacy (pp. 1-6). DOI: 10.1109/EuroSP.2015.12.

[4] Fung, B. C. M., Wang, K., Chen, R. y Yu, P. S. (2018). *A critical evaluation of the article 29 working party's .ºpinion 05/2014 on anonymisation techniques"*. IEEE Transactions on Knowledge and Data Engineering, 30(9), 1847-1852. DOI: 10.1109/TKDE.2018.2812202.

[5] Dwork, C. (2008). *Differential privacy: A survey of results*. En International Conference on Theory and Applications of Models of Computation (pp. 1-19). DOI: 10.1007/978-3-540-79228-4_1.

[6] Revollo Fernández, D. (2017). *El derecho al olvido en Internet a la luz de la jurisprudencia del Tribunal de Justicia de la Unión Europea: el caso Google Spain*. Opinión Jurídica, 16(31), 79-99. DOI: 10.22395/ojum.v16n31a4.