Privacidad digital

y redes descentralizadas

Por qué el modelo importa y qué cambia
cuando la red no depende de una sola empresa

fedipunk.com · tuiter.rocks

Qué entendemos por privacidad en redes sociales

Cuando hablamos de privacidad en redes sociales no hablamos solo de si alguien puede leer tus mensajes:

Qué se recoge	Qué datos genera tu uso de la plataforma, más allá de lo que publicas voluntariamente.
Quién tiene acceso	La empresa, los anunciantes, los algoritmos, los administradores de cada servidor.
Cómo se usa	Para mostrarte publicidad, para perfilarte, para predecir tu comportamiento o para vendérselo a terceros.
Cuánto control tienes	Si puedes borrar tu cuenta de verdad, llevarte tus datos o elegir con quién los compartes.
Quién decide las normas	Si las normas las establece una empresa unilateralmente o hay más actores con más poder distribuido.

Privacidad no es secretismo

«No tengo nada que ocultar» es el malentendido más frecuente sobre la privacidad.

Privacidad no es ocultar

Cierras la puerta de casa no porque hagas algo malo, sino porque decides quién entra y cuándo. Eso es privacidad.

Los datos se usan aunque no hayas hecho nada malo

Se usan para perfilarte, para venderte cosas, para predecir tu comportamiento. No hace falta haber cometido ningún delito para que te afecte.

Es una cuestión de poder y de contexto

Lo que compartes con tu médica no debería llegar a tu jefe. Lo que publicas entre amigos no debería usarse para mostrarte publicidad de seguros. El problema no es el dato: es el control sobre él.

El modelo de negocio que lo cambia todo

Las grandes plataformas sociales son gratuitas porque el producto no es la plataforma:

El modelo es: captar atención → recoger datos de comportamiento → vender acceso a audiencias perfiladas a anunciantes.

El algoritmo no es neutral

Está optimizado para que pases más tiempo en la plataforma, no para que estés bien informada o tengas conversaciones de calidad. El tiempo de conexión es el objetivo.

Las normas sirven al negocio

Las decisiones de moderación, los cambios de algoritmo y las condiciones de uso se toman pensando en el modelo de negocio, no en el bienestar del usuario.

Tus datos son el inventario

No solo lo que publicas: tus patrones de uso, tus interacciones, tu red de contactos, el tiempo que pasas en cada tipo de contenido. Todo esto tiene valor comercial.

La dependencia es deliberada

Si te vas, pierdes tu red y tu historial. Eso no es un accidente: es un diseño. Cuanto más difícil sea irte, mejor para la plataforma.

Qué datos generas aunque no publiques mucho

No hace falta ser activo para dejar huella. Estas señales se recogen solo por usar la plataforma:

⏱️ Tiempo de uso

Cuánto tiempo pasas en la app, a qué horas, con qué frecuencia vuelves.

👁️ Lo que miras, no solo lo que tocas

Cuánto rato te quedas mirando un contenido aunque no des like ni compartas.

🔗 Tu red de contactos

A quién sigues, quién te sigue, con quién interactúas. Eso revela más de ti que cualquier publicación.

📍 Contexto de acceso

Dispositivo, navegador, ubicación aproximada, operador de red.

🔄 Patrones de comportamiento

A qué reaccionas, qué te genera respuesta emocional, qué tipos de contenido te detienen el scroll.

🧩 Lo que no haces

En qué contenidos no participas, qué cosas evitas. La ausencia también es un dato.

Qué pasa cuando una sola empresa controla la red

Más allá de la publicidad, la concentración de poder tiene consecuencias concretas:

1	**Normas que cambian sin previo aviso**	Lo que hoy es aceptable mañana puede no serlo. Y viceversa. No tienes voz en esa decisión.
2	**Moderación inconsistente o arbitraria**	Cuentas cerradas sin explicación. Contenido eliminado sin criterios claros. Poco o ningún recurso.
3	**Cambios de algoritmo que afectan tu visibilidad**	Tu presencia depende de decisiones que no controlas y que pueden cambiar en cualquier momento.
4	**Datos que no puedes recuperar ni borrar del todo**	El 'borrar cuenta' no garantiza que los datos desaparezcan. Las condiciones de uso suelen ser muy amplias.
5	**Dependencia sin alternativa real**	Si te vas, pierdes tu red. Si te quitas, pierdes tu historial. La salida está diseñada para ser cara.

Qué significa que una red sea descentralizada

La analogía del correo

Tienes cuenta en Gmail.
Tu amiga tiene cuenta en Outlook.
Os podéis escribir sin problema.

Nadie controla todo el correo.
Cada proveedor gestiona sus propios servidores y sus propias normas.
Pero todos usan el mismo protocolo.

En el Fediverse pasa lo mismo:
no hay un servidor único ni
una empresa que lo controle todo.

En términos de privacidad:

- No hay una sola empresa recogiendo todos tus datos
- No hay un único algoritmo central para toda la red
- En Mastodon no hay publicidad conductual en el software base
- Las normas las decide cada instancia, no una empresa global
- Puedes elegir en qué servidor confías y quién lo administra

Qué aporta Mastodon como modelo distinto

Mastodon no resuelve todos los problemas de privacidad, pero cambia el modelo de raíz:

🚫 **Sin publicidad conductual por defecto**	El software base de Mastodon no incluye publicidad ni sistema de perfilado comercial. El modelo de negocio no depende de venderte a anunciantes.
⏱️ **Sin algoritmo de engagement**	El timeline es cronológico por defecto. Ves lo que publican quienes sigues, en orden de tiempo. Nada decide por ti qué te conviene ver.
🏛️ **Sin una sola empresa que lo controle todo**	El Fediverse está formado por miles de servidores independientes. No hay un único punto de decisión sobre normas, datos o visibilidad.
📦 **Portabilidad real**	Puedes migrar tu cuenta a otra instancia conservando tus seguidores. Si no te convence tu instancia, puedes irte sin perder toda tu red.
👁️ **Puedes saber quién administra tu instancia**	A diferencia de las grandes plataformas, en una instancia pequeña sabes quién tiene acceso técnico a los datos. Eso permite una relación de confianza más directa.

Lo que mejora y lo que no mejora

Lo que mejora

✓ No hay perfilado comercial ni publicidad conductual

✓ No hay algoritmo central optimizando tu atención en toda la red

✓ Puedes elegir una instancia con normas que confíes

✓ Más control sobre qué ves y quién te ve

✓ Portabilidad: puedes migrar sin perder toda tu red

Lo que no mejora solo

→ Los mensajes directos siguen siendo accesibles para el admin

→ Tus publicaciones públicas son públicas en todo el Fediverse

→ La seguridad de tu cuenta depende de tu contraseña

→ La calidad de la moderación varía entre instancias

→ Tus hábitos de uso importan igual que en cualquier red

Privacidad en Mastodon: expectativas realistas

Mastodon ofrece un modelo más respetuoso con la privacidad, pero no equivale a comunicación anónima ni a mensajería cifrada:

✓	**No hay publicidad conductual en el software base**	Mastodon no incluye sistema de perfilado ni monetización por publicidad. Las instancias pueden añadir donaciones o suscripciones, pero no publicidad conductual.
✓	**Los datos no están centralizados en una sola empresa**	Cada instancia gestiona sus propios datos de forma independiente. No existe una base de datos central con todos los usuarios del Fediverse. Elegir instancia importa.
⚠	**Tu instancia puede ver tus datos técnicos**	El administrador de tu instancia tiene acceso técnico a tus publicaciones, mensajes directos y datos de cuenta. Por eso elegir bien la instancia importa.
⚠	**Los mensajes directos no son mensajería cifrada**	Son visibles solo para quienes participan en la conversación, pero el administrador de tu instancia puede acceder técnicamente. Para comunicación sensible, usa Signal u otra app con cifrado de extremo a extremo.
→	**Lo que publicas como público es público en todo el Fediverse**	Las publicaciones marcadas como públicas pueden aparecer en cualquier instancia federada. No hay un 'solo mis seguidores' en el sentido de Twitter sin ajustar la visibilidad.

Límites y riesgos que siguen existiendo

El Fediverse no es un entorno de anonimato ni de seguridad garantizada. Estos riesgos son reales:

⚠ La instancia que eliges importa mucho

Una instancia mal administrada, sin política de privacidad clara o con un administrador poco fiable puede representar un riesgo real. No todas las instancias son iguales.

⚠ Las publicaciones públicas son indexables

Las publicaciones públicas pueden aparecer en motores de búsqueda, en otras instancias y en archivos de terceros. Si publicas algo como público, puede permanecer aunque lo borres.

⚠ Los metadatos siguen existiendo

Hora de publicación, frecuencia de uso, red de contactos. Aunque el software no los use para publicidad, existen y pueden ser accesibles.

⚠ La federación tiene límites de visibilidad

Algunas instancias bloquean a otras por razones de moderación. El contenido no fluye de forma completamente simétrica ni predecible.

Prácticas que ayudan dentro del Fediverse

1. **Elige una instancia con política de privacidad clara**

   Antes de registrarte, lee quién la administra y cómo gestiona los datos.

2. **Configura la visibilidad de tus publicaciones**

   Mastodon permite publicar solo para seguidores, solo para menciones o de forma pública. Úsalo de forma consciente.

3. **No uses mensajes directos para comunicaciones sensibles**

   Para conversaciones confidenciales, usa Signal u otra app con cifrado de extremo a extremo.

4. **Revisa qué aplicaciones tienen acceso a tu cuenta**

   Si has conectado apps de terceros, revísalas periódicamente y revoca acceso a las que ya no uses.

5. **Aplica el mismo criterio que en cualquier red**

   No publiques información que no quieras que sea permanente o accesible. El contexto importa.

6. **Usa una contraseña única y activa la autenticación en dos pasos**

   La seguridad de tu cuenta no es específica del Fediverse, pero es el primer paso.

Por dónde empezar sin agobiarse

No hace falta hacer todo a la vez. Estos pasos son suficientes para empezar:

1	**Elige una instancia con registro abierto y política de privacidad clara**	fedipunk.com/instancias-mastodon-espanol
2	**Usa una contraseña única y activa la verificación en dos pasos si la instancia lo permite**	Es el primer paso de seguridad básica en cualquier servicio
3	**Configura la visibilidad por defecto de tus publicaciones**	Decide si quieres que tus publicaciones sean públicas por defecto o solo para seguidores
4	**No uses mensajes directos para comunicación sensible**	Para eso: Signal u otra aplicación con cifrado de extremo a extremo
5	**Sigue a personas activas y preséntate con #NuevoEnMastodon**	La privacidad no significa aislamiento. La comunidad es parte del valor de la red

Recursos para empezar en español

Guía central de Mastodon y el Fediverse

tuiter.ovh/guia-mastodon-fediverso

Guía completa en español: qué es Mastodon, cómo funciona, cómo elegir instancia y los primeros pasos.

Directorio de instancias en español

fedipunk.com/instancias-mastodon-espanol

Un buen punto de partida para explorar instancias activas en español y elegir dónde empezar.

Tuiter.rocks

tuiter.rocks

Instancia de Mastodon en español con comunidad activa y registro abierto.

FediPunk

fedipunk.com

Recursos, directorio y artículos sobre Mastodon y el Fediverse en español.

La privacidad no es un problema técnico.

Es una pregunta sobre quién toma las decisiones.

El modelo que usas para comunicarte forma parte de esa respuesta.

Preguntas

fedipunk.com
tuiter.rocks