¿Qué tan privado es su tomador de notas con IA?

Los tomadores de notas con IA convierten su reunión en un registro en manos de terceros. Descubra qué sale en cada paso, cómo comprobar las afirmaciones de una herramienta y cómo mantenerlo todo en local.

Publicado por Julian Pscheid · 15 de julio de 2026 · Actualizado 20 de agosto de 2026
Leer este artículo en línea: https://www.hedy.ai/es/post/how-to-use-ai-meeting-notes-privately/

Dos colegas conversan en una mesa pequeña dentro de un despacho privado con la puerta cerrada; entre ellos hay un iPhone boca abajo junto a un cuaderno y una taza con forma de pato de los Oregon Ducks

Respuesta rápida Un tomador de notas para reuniones con IA hace tres cosas que pueden filtrar datos por separado: transcribe el audio, analiza la transcripción y almacena el resultado. La mayoría de las herramientas ejecutan las tres en sus propios servidores, por lo que la reunión se convierte en un registro consultable en manos de terceros. Unas pocas pueden ejecutar las tres en hardware que usted posee, la única configuración en la que nada sobre la reunión sale de la sala. Hedy transcribe en el dispositivo por defecto en todas las plataformas para las que está disponible y, en la mayoría del hardware actual, también puede ejecutar el análisis en el dispositivo. Si además desactiva Cloud Sync de Hedy, nada de la conversación llega a nuestros servidores a menos que comparta explícitamente esa sesión.

The Associated Press publicó este mes un artículo sobre los tomadores de notas con IA en el trabajo que cataloga bien los riesgos (AP, julio de 2026 (https://apnews.com/article/ai-notetaker-work-meetings-privacy-data-c700299371ca7cfec77dafdfb948067f)): información confidencial del personal, estrategia corporativa, secretos comerciales y comentarios que más adelante dejan una mala impresión en una

declaración judicial. Sus consejos también son sensatos. Compruebe si se ha unido un tomador de notas. Pida consentimiento antes de una reunión delicada. Apóyese en la política de la empresa para que ninguna persona tenga que ser quien se oponga. Desactive la herramienta durante la parte delicada. Pregunte qué conserva el proveedor y si usa algo de ello para entrenar modelos.

Cada una de esas medidas gestiona las consecuencias de que su reunión se convierta en un registro en manos de terceros. Ninguna pregunta si tiene que convertirse en uno. Justin Daniels, abogado corporativo de Baker Donelson, ofreció la frase más contundente del artículo: «No empezaré a hablar de nada sustancial hasta que se haya desactivado, porque sencillamente no quiero asumir el riesgo». Es el consejo adecuado para las herramientas que usa la mayoría de las personas, y parte de la premisa de que la reunión tiene que salir de su hardware.

En los dispositivos actuales, no tiene por qué hacerlo. Un reducido número de productos puede ejecutar todo el flujo en su propia máquina, y casi nadie lo sabe.

¿Qué sale cuando usa un tomador de notas?

Tres cosas, y pueden filtrarse por separado. La transcripción convierte el audio en texto. El análisis lee ese texto y redacta el resumen y las tareas pendientes. El almacenamiento determina si algo de ello persiste en algún lugar que usted no controla. Cada uno puede permanecer en hardware que usted posee o trasladarse al de terceros, lo que da lugar a ocho combinaciones posibles.

Paso	Qué hace	¿Puede ejecutarse en el dispositivo?	Qué sale si no lo hace
Transcripción	Convierte el audio en texto, a veces con etiquetas de hablante	Sí, en hardware actual	El propio audio, además de una incrustación acústica por hablante en muchos sistemas
Análisis	Lee la transcripción y redacta resúmenes y tareas pendientes	Sí, en hardware con capacidad suficiente	La transcripción y todo lo que un modelo infiera de ella
Almacenamiento y sincronización	Conserva el archivo	Sí, si se mantiene desactivado	Una copia duradera y consultable, además de metadatos que pueden sobrevivir a la eliminación

Aquí es donde se esconden la mayoría de las afirmaciones sobre privacidad. «El audio nunca sale de su dispositivo» suena como una declaración sobre todo el producto. Solo significa que la transcripción es local, y es compatible con enviar la transcripción literal completa a un modelo de lenguaje un segundo después. Hedy hace exactamente eso por defecto, por lo que «¿sale el audio?» es la pregunta equivocada para detenerse. La transcripción es el registro. Una vez que sale de su máquina, casi todo lo que le preocupaba ya ha salido de ella.

El procesamiento híbrido es habitual, incluida la configuración predeterminada de Hedy. El problema es un proveedor que no dice qué pasos salen de su dispositivo.

Diagrama que compara la mayoría de los tomadores de notas, en los que el audio se envía a los servidores del proveedor y la transcripción, el análisis y el almacenamiento se ejecutan allí, con una configuración completamente local en la que los tres pasos se ejecutan en su propio dispositivo

¿Puede ejecutarse todo el flujo en su dispositivo?

Sí, en hardware actual, y esta es la parte que ha cambiado discretamente. Muy pocos productos realizan los tres pasos.

La transcripción es el paso más sencillo

Whisper, el motor predeterminado, se ejecuta en todas las plataformas para las que Hedy está disponible. Nemotron se ejecuta en todas las plataformas nativas, pero no en la aplicación web. Nemotron es un motor de streaming basado en el modelo de voz de 600 millones de parámetros de NVIDIA (https://huggingface.co/nvidia/nemotron-3.5-asr-streaming-0.6b) , y añade las etiquetas de hablante que antes llevaban a muchas personas a elegir un motor en la nube. Requiere una descarga única de aproximadamente 0,6 a 0,7 GB y hardware de la generación del iPhone 12 en adelante. La precisión sigue variando según el acento, el ruido de la sala, el habla superpuesta y el vocabulario especializado, así que pruébelo en sus propias reuniones en vez de confiar en cualquier cifra publicada.

El análisis es donde está la contrapartida

El Procesamiento de IA local (/es/help/local-ai-processing/) ejecuta los resúmenes y las sugerencias en su máquina, y requiere hardware de verdad: un Mac con Apple Silicon, un PC con Windows y una GPU con capacidad suficiente, o un iPhone o iPad reciente. Los modelos van desde unos 1,2 GB para el nivel móvil hasta más de 20 GB. Un modelo de nivel intermedio de unos 9 mil millones de parámetros funciona con holgura en un Mac de 16 GB. Los más grandes necesitan alrededor de 25 GB de RAM o más.

El Procesamiento de IA local está desactivado por defecto porque el análisis en la nube es más rápido y, por ahora, produce mejores resultados. La configuración predeterminada de Hedy es una división deliberada: reconocimiento de voz local en todas partes para que el audio nunca salga sin que usted lo solicite, y análisis en la nube para que el producto funcione bien en hardware que no puede alojar un modelo de lenguaje. Un resumen que parece instantáneo en la nube puede tardar entre treinta segundos y varios minutos en local. El análisis técnico profundo (/es/post/local-ai-engineering-deep-dive-hedy-3-2/) ofrece todos los detalles.

El Procesamiento de IA local no recurre silenciosamente a la nube. Si algo falla localmente, usted recibe un error, no un reintento silencioso contra un servidor. Recurrir a la nube sin avisar es la peor propiedad que puede tener una función de privacidad, porque falla precisamente en la dirección que usted trataba de evitar y no le dice nada.

El almacenamiento es un interruptor, no una función

El paso que las personas olvidan es el archivo, porque llega disfrazado de comodidad. Cloud Sync copia los datos de la sesión en los servidores de Hedy para que sus otros dispositivos puedan verlos. Déjelo activado y tendrá acceso entre dispositivos con procesamiento local. Desactívelo y nada de la conversación llegará a nuestros servidores a menos que comparta explícitamente esa sesión. El procesamiento local y el almacenamiento local son decisiones distintas, y una herramienta que solo ofrece el primero no ha cerrado el flujo.

¿Cómo comprueba las afirmaciones de un tomador de notas?

Observe el comportamiento y después lea los documentos. Ninguna de las dos cosas basta por sí sola.

Pruebe el modo avión. Desactive la red e inicie una sesión. Si una herramienta sigue transcribiendo y resumiendo, existe una ruta local, y conviene saberlo. Considérelo una señal, no una prueba concluyente: que se detenga puede significar que la herramienta requiere iniciar sesión o descargar un modelo en vez de necesitar la nube, y una herramienta con una ruta sin conexión que funciona puede seguir enviando todo a un servidor en cuanto usted vuelve a conectarse. Le indica que existe un modo local. No le dice qué ocurre cuando está conectado.

Preste atención a la cuestión de las etiquetas de hablante. Si una herramienta muestra etiquetas de hablante y afirma que nada sale de su dispositivo, pregunte qué motor en el dispositivo realiza la diarización. Un proveedor capaz de nombrarlo le está aportando información real. Uno que no puede hacerlo quizá esté etiquetando en el servidor.

Lea la lista de subprocesadores. La política de privacidad está redactada para tranquilizar. La lista de subprocesadores existe para las compras y los avisos contractuales, por lo que nombra a las empresas que participan en el flujo. La de Hedy contiene dieciséis entradas en trust.hedy.ai (https://trust.hedy.ai) . Consulte la lista de cualquier proveedor para saber qué empresas pueden recibir el contenido de la reunión y por qué; la longitud por sí sola dice poco.

Pregunte qué sobrevive a la eliminación. Danielle Kays, socia de Fisher Phillips, señaló que los metadatos de la reunión pueden persistir en poder de un proveedor después de eliminar el contenido, y que en algunos casos un modelo puede memorizar o reproducir el contenido ingerido. El significado de «eliminar» varía según el proveedor y a menudo quiere decir «quitar de la vista que usted puede ver».

Si de verdad importa, inspeccione el tráfico. Las pruebas sin conexión y las páginas de privacidad responden a preguntas distintas, y ninguna observa la red. Para un despliegue regulado, la inspección de paquetes o DNS es la comprobación que observa realmente lo que envía una herramienta.

¿Qué debería preguntar antes de instalar uno?

Cinco preguntas. La respuesta a cada una debe ser concreta.

1. ¿Dónde se ejecuta cada uno de los tres pasos? Transcripción, análisis y almacenamiento, nombrados por separado. No «¿es privado?».

2. ¿Crean etiquetas de hablante y dónde? Si se generan en el servidor, pregunte qué es la incrustación, cuánto tiempo se conserva y qué aviso reciben los participantes.

3. ¿Cuál es el calendario de conservación y destrucción? Por escrito y con un plazo. Illinois exige exactamente esto y, según los abogados citados más adelante, la mayoría de las empresas que despliegan estas herramientas no lo tienen.

4. ¿Quiénes son los subprocesadores y dónde están? Esta es también la pregunta del RGPD (/es/post/gdpr-checklist-ai-meeting-tools/) si tiene participantes europeos, un contexto en el que los acontecimientos recientes sobre las transferencias UE-EE.UU. (/es/post/eu-us-data-transfers-supreme-court-ftc-ruling/) han hecho que la base jurídica resulte menos cómoda que antes.

5. ¿Recurre a la nube cuando falla y lo avisa? Recurrir silenciosamente a la nube convierte una configuración de privacidad en un adorno.

¿Cómo ejecuta Hedy sin que nada salga?

Compruebe una opción predeterminada y luego cambie dos ajustes.

Abra Settings !’ Speech & AI . Confirme que esté seleccionado Whisper o Nemotron. Whisper ya es la opción predeterminada, así que la mayoría de las personas descubrirá que esto ya está hecho; solo necesita tocarlo si alguien cambió a un proveedor en la nube.

En la misma pantalla, active Local AI Processing y elija un modelo que muestre la etiqueta «Great fit». Hedy comprueba la memoria disponible y marca cada modelo como Great fit, Tight fit o Won't fit, para que usted no tenga que adivinar. Se configura por dispositivo, así que su Mac y su iPhone necesitan cada uno su propia configuración.

Después, desactive Cloud Sync . Con esta función desactivada, ningún dato de la reunión llega a nuestros servidores a menos que comparta explícitamente una sesión.

Si su hardware no puede ejecutar un modelo local, el control de privacidad de Cloud AI Analysis (/es/help/cloud-ai-analysis-privacy-control/) es la opción intermedia: detiene el análisis en la nube mientras la transcripción local sigue funcionando, de modo que obtiene una transcripción privada sin notas generadas por IA. Nuestra guía de configuración (/es/post/ai-meeting-privacy-settings-explained/) explica la matriz completa y la página de seguridad (/es/security/) documenta cada configuración.

¿Un tomador de notas privado sigue necesitando consentimiento?

Sí. Una herramienta basada en el dispositivo es más difícil de ver para otras personas que un bot.

AP señaló que los participantes pueden usar dispositivos personales para tomar notas separados de la plataforma de reuniones, «en cuyo caso los demás asistentes no sabrían necesariamente que se estaba grabando y transcribiendo una conversación». Un bot se muestra en la lista de asistentes. Una app en el teléfono de alguien no muestra nada. Eso facilita la grabación discreta, y es una crítica justa a la categoría en la que estamos. Thorin Klosowski, analista sénior de seguridad y privacidad de la Electronic Frontier Foundation, dio la respuesta directa: «Pedir el consentimiento de todos antes de celebrar una

reunión delicada sería la forma más educada de proceder».

El procesamiento local determina adónde van los datos. No dice nada sobre si alguien dio su consentimiento. Las leyes de grabación, las políticas del lugar de trabajo y los deberes profesionales siguen vigentes con independencia de la arquitectura, y usar una herramienta que nadie puede ver aumenta la obligación de comunicarlo.

Lo que sí se vuelve más fácil es la conversación. La mayor parte de la resistencia a ser grabado no se debe a las notas, sino al archivo: quién más lo ve, cuánto tiempo se conserva, qué ocurre si otra empresa adquiere al proveedor. «Se queda en mi portátil y lo eliminaré después» da lugar a una conversación distinta de «se está subiendo a un servicio cuyas condiciones no he leído». Escribimos guiones de consentimiento palabra por palabra (/es/post/ask-permission-to-record-meeting-consent-scripts/) para la versión incómoda, y nuestro artículo sobre leyes de grabación y consentimiento (/es/help/recording-laws-and-consent/) cubre el aspecto jurisdiccional.

Chris Pluymers, abogado asociado de The Dillon Law Group, también propuso una frase para rechazar un tomador de notas: «Prefiero que mantengamos esta reunión sin herramientas de grabación ni transcripción con IA, y con gusto puedo tomar mis propias notas y compartir un resumen si resulta útil». Amy Dufrane, directora ejecutiva del organismo de certificación de RR. HH. HRCI, sugirió que la objeción fuera institucional en lugar de personal y que se citara la política de la empresa para que ninguna persona tuviera que ser quien se opusiera.

¿Por qué son las transcripciones más arriesgadas que las grabaciones?

Klosowski hizo la observación más incisiva del artículo de AP: «Almacenar un montón de vídeo no es fácil, es costoso y difícil de revisar, pero el texto es mucho más fácil de buscar y más barato de almacenar».

Antes de los tomadores de notas con IA, la protección práctica de una grabación era la fricción. Una reunión de dos horas es un objeto de dos horas. Nadie la recorre sin un motivo, y el almacenamiento cuesta lo suficiente para que las grabaciones se eliminen. Esa fricción realizaba una verdadera labor de seguridad que nadie tenía que presupuestar.

Las transcripciones la eliminan. El texto es tan barato que se puede conservar para siempre y permite búsquedas desde el momento en que se almacena. Una sola consulta en cuatro años de archivos muestra cada aparición de una frase a cualquiera que tenga acceso, incluido el abogado de la parte contraria con una orden de exhibición de pruebas. Un comentario que habría muerto en una grabación que nadie vio se convierte en un resultado de búsqueda.

Pero no es un aumento inequívoco del peligro. El audio contiene elementos que el texto pierde: el tono, la conversación de fondo y una muestra suficiente de su voz como para clonarla. Además, el audio se puede transcribir más adelante, por lo que una grabación es una transcripción que todavía no se ha producido. El cambio va de «alguien podría encontrar esto» a «alguien puede encontrar esto al instante», y la mayoría de las personas nunca tuvo en cuenta la diferencia.

¿Qué es una huella de voz y quién tiene la suya?

Pluymers describió el mecanismo: para distinguir al Hablante 1 del Hablante 2, muchos tomadores de notas derivan una firma acústica de cada voz. Ese proceso se llama diarización, y es el hilo que la mayoría de los lectores no habrá considerado.

Situación actual de la ley

En Illinois, las huellas de voz son identificadores biométricos en virtud de la Biometric Information Privacy Act, que exige un aviso por escrito, la divulgación de la finalidad y el plazo de conservación, una autorización firmada antes de la recopilación y un calendario de destrucción documentado (740 ILCS 14/15 (https://www.ilga.gov/ftp/ILCS/Ch%200740/Act%200014/074000140K15.html)). Que una incrustación de diarización cuente como una de ellas es una teoría emergente que se está poniendo a prueba en los tribunales, no una cuestión jurídica resuelta (Lewis Rice (https://www.lewisrice.com/publications/ai-transcription-tools-give-rise-to-bipa-claims)). Algunos diarizadores de extremo a extremo ni siquiera funcionan así, sino que asignan el audio a índices anónimos de hablantes sin crear una plantilla persistente.

Los litigios son reales. Las herramientas de IA para reuniones son un objetivo activo de demandas colectivas en virtud de BIPA (Fisher Phillips (https://www.fisherphillips.com/en/insights/insights/ai-meeting-tools-are-the-latest-target-of-illinois-bipa-class-actions)), y Fireflies.ai es la demandada en una supuesta demanda colectiva que alega que graba, transcribe y almacena las voces de los participantes, incluidas personas que nunca se registraron, sin el aviso, el consentimiento y las salvaguardas de conservación exigidos (Jackson Lewis (https://www.workplaceprivacyreport.com/2026/04/articles/artificial-intelligence/ai-meeting-assistants-and-biometric-privacy-governance-lessons-from-the-fireflies-ai-lawsuit/)). Son alegaciones y ningún tribunal se ha pronunciado sobre el fondo.

Lo que una huella de voz robada puede y no puede hacer

La versión alarmista circula, así que conviene corregirla: una incrustación de diarización robada no es una llave para acceder a su cuenta bancaria. Los bancos registran sus propias plantillas de voz, y la incrustación interna de un proveedor no es intercambiable con ellas. El riesgo real de la voz es más corriente, y basta con tener suficiente audio grabado para clonar a alguien de forma convincente (FTC (https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/approaches-address-ai-enabled-voice-cloning)). Ese es un argumento sobre el audio, no sobre la incrustación.

Por qué la diarización en el dispositivo cambia la exposición

La diarización en el dispositivo cuenta con un precedente útil. En Barnett v. Apple , un tribunal de apelaciones de Illinois confirmó la desestimación de una demanda colectiva en virtud de BIPA por Face ID y Touch ID, al determinar que Apple ni poseía ni recopilaba los datos biométricos de los usuarios porque nunca salían de sus propios dispositivos, nunca se enviaban a los servidores de Apple y las funciones eran opcionales y se podían eliminar (Duane Morris (https://blogs.duanemorris.com/classactiondefense/2023/01/09/illinois-appellate-court-affirms-dismissal-of-bipa-class-action-lawsuit/) , IAPP (https://iapp.org/news/b/court-rules-apples-facial-fingerprint-tools-comply-with-bipa)). Esto se corresponde estrechamente con la diarización local: se deriva en su dispositivo, nunca se transmite, es opcional y se puede eliminar. El motor Nemotron (/es/post/nemotron-on-device-speech-engine/) de Hedy funciona así.

No es un puerto seguro. Barnett dependió de sus hechos; un diseño o unos alegatos distintos podrían producir un resultado diferente, y no dice nada sobre las obligaciones de quien convocó la reunión. Esto es una reducción del riesgo respaldada por un buen precedente, y nada de ello constituye asesoramiento jurídico.

¿Puede un tomador de notas afectar al privilegio abogado-cliente?

Un tribunal federal ha determinado que los documentos generados por IA no estaban protegidos por el privilegio.

Lo que determinó el tribunal

En United States v. Heppner , el juez Jed Rakoff del Southern District of New York determinó en febrero de 2026 que los documentos que un acusado penal produjo al introducir información de sus abogados en un chatbot no estaban protegidos ni por el privilegio abogado-cliente ni por la doctrina del producto del trabajo jurídico. La herramienta generó 31 documentos a partir de sus indicaciones, incluido un esquema de su propia estrategia de defensa (Harvard Law Review (https://harvardlawreview.org/blog/2026/03/united-states-v-heppner/)). Rakoff dio tres razones: el chatbot «claramente no es un abogado»; sus propios descargos de responsabilidad advertían que no se debía tratar el resultado como asesoramiento jurídico, lo que debilitaba cualquier afirmación de que el asesoramiento jurídico era la finalidad predominante; y la política de privacidad publicada por el proveedor advertía que la información del usuario podía compartirse en litigios, de modo que el usuario no tenía una expectativa razonable de privacidad (Dorsey (https://www.dorsey.com/newsresources/publications/client-alerts/2026/2/ai-attorney-client-privilege)).

La razón intermedia merece una segunda lectura. La política de privacidad no fue la defensa. Fue la prueba. El documento que el proveedor redactó para describir sus propias prácticas de datos se convirtió en la razón por la que la expectativa de confidencialidad del usuario no era razonable.

Hasta dónde se aplica

Heppner no decidió si un tomador de notas para reuniones implica una renuncia al privilegio. Se refería a un acusado que usó un chatbot por iniciativa propia, no a una herramienta presente en una conversación privilegiada, y los expertos todavía están analizando qué significa para los tomadores de notas (Columbia Blue Sky (https://clsbluesky.law.columbia.edu/2026/06/16/cahill-discusses-a-i-note-takers-in-corporate-meetings/)). El New York City Bar tiene una opinión formal sobre la ética de usar IA para grabar y transcribir conversaciones con clientes que trata la grabación y la conservación como problemas separados (NYC Bar Formal Op. 2025-6 (https://www.nycbar.org/reports/formal-opinion-2025-6-ethical-issues-affecting-use-of-ai-to-record-transcribe-and-summarize-conversations-with-clients/)).

Su advertencia más concreta sí se traslada: enviar material confidencial a un tercero puede debilitar la expectativa de que siga siendo confidencial. Un flujo sin terceros no plantea esa cuestión. Tampoco crea privilegio, impide la exhibición de pruebas ni convierte en adecuada una conversación grabada de forma indebida. Daniels expresó la versión práctica con claridad: «si los datos van a cualquier otro lugar y ellos no lo saben, esa conversación protegida por el privilegio abogado-cliente podría dejar de estar protegida».

¿Qué reuniones necesitan una configuración completamente local?

No todas, y fingir lo contrario hace que el consejo sea fácil de descartar.

Para una reunión semanal de seguimiento, la configuración predeterminada en la nube está bien. Vale la pena aceptar un resumen más lento con una configuración completamente local cuando la propia transcripción representa el riesgo: consultas jurídicas, investigaciones de RR. HH., reuniones del consejo y negociaciones, entrevistas con fuentes en las que un nombre en una transcripción puede costarle el trabajo a alguien, y pacientes que graban sus propias citas médicas para repasar después lo que dijo el médico. Si quiere una visión más amplia de las herramientas en el dispositivo más allá de las reuniones, comparamos siete herramientas de IA local (/es/post/best-local-ai-tools-for-productivity/) .

La elección adecuada se hace por reunión, no por persona. La mayoría de las reuniones puede usar la configuración predeterminada en la nube. Para las pocas en las que la propia transcripción sería perjudicial, use una configuración completamente local, verifíquela antes de la llamada y diga qué está usando.

Preguntas frecuentes

¿Puede usar un tomador de notas con IA sin enviar nada a la nube?

Sí, pero solo con el reducido número de herramientas capaces de ejecutar cada paso en su hardware. Un tomador de notas transcribe el audio, analiza la transcripción y almacena el resultado. Cada una de esas etapas puede filtrar datos por separado, y la mayoría de las herramientas ejecutan las tres en servidores de terceros. Hedy transcribe en el dispositivo por defecto en todas las plataformas para las que está disponible y, en la mayoría del hardware actual, también puede ejecutar el análisis en el dispositivo. Con Cloud Sync desactivado, ningún dato de la reunión llega a nuestros servidores a menos que comparta explícitamente una sesión.

¿Basta con comprobar que el audio nunca sale de mi dispositivo?

No, y este es el error más común. «El audio nunca sale» solo indica que la transcripción es local, que es uno de tres pasos. Una herramienta puede transcribir en su dispositivo y aun así enviar la transcripción a un modelo de lenguaje, que es exactamente lo que Hedy hace por defecto. La transcripción es el registro literal, por lo que enviarla fuera del dispositivo plantea casi todas las mismas preguntas que plantearía el audio. Pregunte por cada paso, no solo por el micrófono.

¿Los tomadores de notas con IA crean huellas de voz de los participantes de una reunión?

Algunos sí, como efecto secundario de etiquetar quién habló. Muchos sistemas de diarización extraen una incrustación acústica de cada voz para distinguir a los hablantes. Que esa incrustación sea una huella de voz regulada por la Illinois Biometric Information Privacy Act es una teoría jurídica que sigue litigándose, no una cuestión resuelta, y no todos los sistemas funcionan así. Lo que usted puede controlar es dónde se realiza el etiquetado: la diarización en el dispositivo no transmite nada.

¿El procesamiento en el dispositivo elimina la exposición en materia de privacidad biométrica?

La reduce, y existe jurisprudencia real que lo respalda. En Barnett v. Apple , un tribunal de apelaciones de Illinois determinó que Apple no poseía ni recopilaba los datos biométricos de los usuarios porque permanecían en sus propios dispositivos, nunca se enviaban a los servidores de Apple y las funciones eran opcionales y se podían eliminar. Es un precedente significativo para el procesamiento local, pero

dependió de esos hechos concretos. Reduce el riesgo, no constituye un puerto seguro, y no dice nada sobre las obligaciones de quien convocó la reunión.

¿Puede una herramienta de IA afectar al privilegio abogado-cliente?

Un tribunal federal ha determinado que los documentos generados por IA no estaban protegidos por el privilegio. En United States v. Heppner , el juez Jed Rakoff concluyó que los documentos que un acusado produjo al introducir información de sus abogados en un chatbot no estaban protegidos ni por el privilegio ni como producto del trabajo jurídico, en parte porque la política de privacidad del proveedor advertía que la información podía compartirse en un litigio. Ese caso se refería a un chatbot que el acusado usó por su cuenta, no a un tomador de notas para reuniones, así que no resuelve la cuestión de estos últimos. Consulte a su propio asesor jurídico.

¿Desactivar Cloud Sync hace que un tomador de notas sea privado?

No por sí solo. La sincronización rige el almacenamiento, no el procesamiento. Una herramienta puede no conservar nada en sus servidores y aun así haber enviado su audio a una API de transcripción y su transcripción a un modelo de lenguaje durante el proceso. El almacenamiento, la transcripción y el análisis son cuestiones distintas, y un proveedor que solo responde a la del almacenamiento no ha respondido a las demás.

¿Cómo comprueba si un tomador de notas se ejecuta localmente?

El modo avión es una primera comprobación útil, pero no es una prueba concluyente. Si una herramienta sigue transcribiendo sin conexión, existe una ruta local. Si se detiene, puede significar que necesita la nube o simplemente que requiere iniciar sesión o descargar un modelo. Además, una herramienta con una ruta local sin conexión puede seguir enviando datos a la nube cuando usted vuelve a conectarse. Combine la prueba sin conexión con la lista de subprocesadores del proveedor y, si de verdad importa, con una inspección de red.

¿La transcripción en el dispositivo es lo bastante precisa para reuniones reales?

Para reuniones cotidianas, funciona bien. El motor Nemotron de Hedy se basa en el modelo de voz en streaming de 600 millones de parámetros de NVIDIA, se ejecuta íntegramente en el dispositivo y etiqueta quién dijo qué. La precisión sigue variando según el acento, el ruido de fondo, el habla superpuesta y el vocabulario especializado, así que pruébelo en sus propias reuniones en vez de confiar en las pruebas comparativas de nadie, incluidas las nuestras.

¿Un tomador de notas basado en el dispositivo es menos transparente que un bot de reunión?

Sí, y eso juega en contra de herramientas como la nuestra. Un bot anuncia su presencia en la lista de asistentes. Una app en el teléfono de alguien no anuncia nada, lo que facilita la grabación secreta en lugar de dificultarla. The Associated Press señaló esto directamente. El procesamiento local aborda adónde van los datos y no hace nada respecto a si las personas dieron su consentimiento. Son deberes distintos y usted sigue teniendo que cumplir el segundo.

¿Qué envía Hedy a la nube por defecto?

El reconocimiento de voz se ejecuta en su dispositivo en todas las plataformas, por lo que el audio no sale por defecto. El paso de análisis que redacta resúmenes y sugerencias se ejecuta en la nube por defecto, donde el contenido de la transcripción se procesa de forma transitoria y no se usa para entrenar modelos. Esta configuración predeterminada es una elección deliberada entre compatibilidad con más dispositivos y calidad de los resultados. Puede trasladar el análisis al dispositivo con el Procesamiento de IA local (/es/help/local-ai-processing/) y desactivar Cloud Sync para que nada se sincronice.

¿El procesamiento local cuesta más?

No. El reconocimiento de voz en el dispositivo y el Procesamiento de IA local forman parte del producto, no de un nivel de privacidad. El nivel gratuito incluye 300 minutos al mes y Pro cuesta $12.99 al mes o $99.99 al año. Los modelos locales se descargan una sola vez en lugar de cobrarse por minuto, por lo que la ruta completamente local no tiene coste de uso. Consulte los precios (/es/pricing/) actuales.

Hedy AI · Coaching de IA en vivo para conversaciones importantes

Prueba Hedy gratis: https://www.hedy.ai/es/downloads/

https://www.hedy.ai/es/post/how-to-use-ai-meeting-notes-privately/