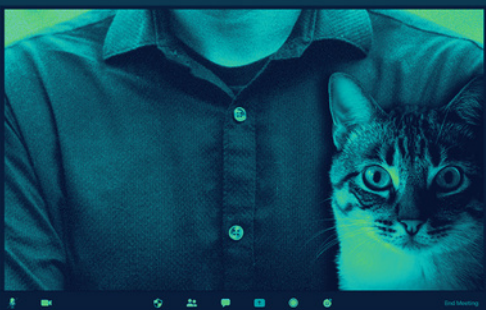


Privacidad en las videollamadas

No todos los participantes son amistosos

Con la reciente pandemia, como reza el cliché, muchas cosas vinieron para quedarse. Algunas más que otras. Habrá quien vuelva a usar mascarilla cuando viaje en un metro atiborrado de gente, quien se compre un perro para poder salir a pasear en caso de que vuelvan las restricciones a la movilidad por otro virus, o quien atesore un gran inventario de papel higiénico. Esto puede darse en algunos casos, pero lo que sí es una herencia popular es el uso de los programas para realizar videollamadas.



Durante la crisis de la COVID se llegaron a organizar desde happy hours virtuales hasta sesudas clases académicas o reuniones laborales a diversas horas y casi todos los días. Esta vorágine puede que se haya frenado, pero en general las videollamadas siguen siendo una herramienta muy utilizada por particulares y empresas. En 2020, el mercado global de

videoconferencias fue valorado en aproximadamente **6.000 millones de dólares** y se proyecta que alcance los 11.600 millones para 2027, con una tasa de crecimiento anual del 9,7 %. Hay muchas posibilidades al alcance –desde aplicaciones fáciles de utilizar hasta sistemas más complejos y acotados– y la oferta de estos servicios no para de crecer.

Todas, absolutamente todas las plataformas, conllevan riesgos para la seguridad. Si no, que se lo digan al Ejército alemán, que a principios de mayo detectó un fallo de ciberseguridad que permitió el acceso externo a información sobre al menos 6.000 videoconferencias



realizadas en el sistema Webex, según detalló la prensa local. Algunas de esas reuniones eran altamente secretas. Alguna trataba sobre sobre los misiles largo alcance. Taurus pedidos por Ucrania y otras sobre el campo de batalla digital.

Las salas de reunión virtuales asignadas a los 248.000 miembros del Ejército alemán eran fáciles de encontrar gracias a una **arquitectura informática simple** y a que no estaban protegidas por contraseña. El medio que reveló el caso afirmó que entre los espacios de videoconferencias comprometidos estaba el de Ingo Gerhartz, el jefe de las Fuerzas Aéreas alemanas. Este ya se había visto involucrado en un escándalo por la interceptación de los servicios de inteligencia rusos de una conversación confidencial entre oficiales de alto rango (uno de ellos no utilizó la conexión segura requerida en Webex).

Lo cierto es que, aunque las plataformas de videollamadas proporcionan advertencias y recursos respecto de los riesgos de privacidad, a menudo **no son suficientes en términos de claridad, accesibilidad y proactividad.**

Por eso, mejorar las notificaciones, ofrecer educación continua y simplificar las opciones de configuración ayudaría a los usuarios a proteger su privacidad de manera más efectiva.

Partiendo de la premisa de que no hay plataforma 100 % segura y de que existe bastante margen para el error o descuido humano, los consumidores solo pueden minimizar los peligros. Para ello, tienen que ser conscientes de que antes de utilizar estos programas deben leer bien la letra pequeña y de que

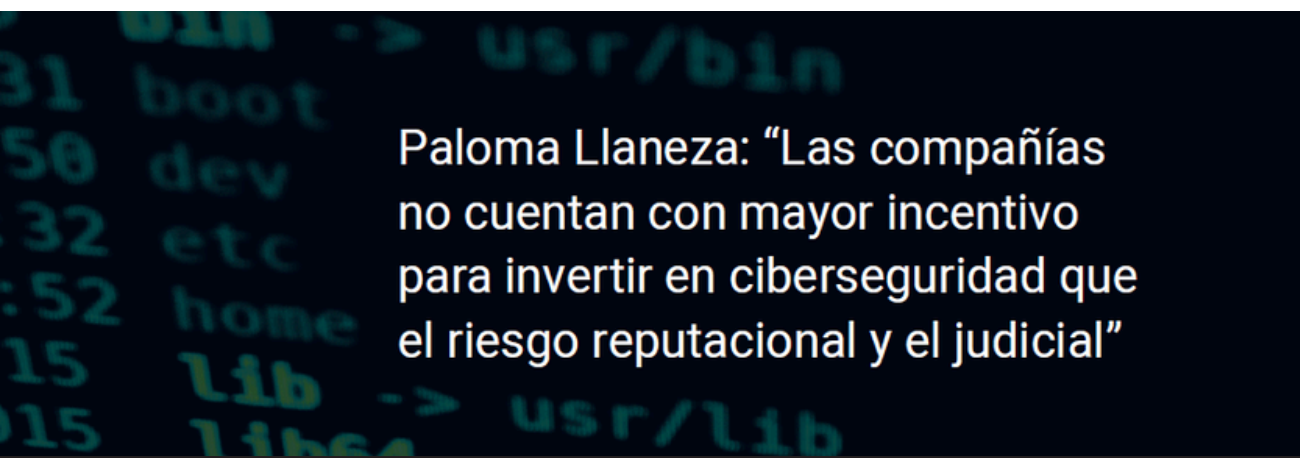
las defensas contra los internautas malintencionados no duran para siempre, por lo que hay que actualizarlas constantemente.

“Las videoconferencias, como cualquier otra actividad digital que dependa de una plataforma para la prestación de un servicio y de una comunicación por redes públicas, requieren estrictas medidas de seguridad para las que no hay más normativa aplicable que el Reglamento General de Protección de Datos y las limitaciones de responsabilidad que las propias plataformas nos hacen aceptar”, asegura Paloma Llaneza, CEO de Razona Legaltech y coordinadora del Comité Editorial de Fundación Hermes.

Inseguridad creciente

Los casos de **violaciones a la privacidad en las videoconferencias** se han disparado en proporción al aumento del uso de esta herramienta en los últimos cinco años. El escándalo más sonado fue sin duda el de Zoom, el sistema que pasó de 10 millones de participantes de reuniones diarios en diciembre de 2019, a 300 millones en abril del año siguiente, ya en plena pandemia. El secreto de su éxito de entonces, y también de su vulnerabilidad, es que era una aplicación fácil de utilizar: bastaba hacer clic en un enlace para hablar con nuestros compañeros de trabajo, alumnos, amigos o familiares.

Zoom no fue honesta con sus usuarios y acabó multada con 85 millones de dólares por dejar al descubierto datos personales que permitieron a terceros irrumpir en las videollamadas. Al respecto, Llaneza destaca que las compañías “no cuentan con mayor incentivo para invertir en ciberseguridad que el riesgo reputacional y las demandas judiciales que se inicien contra ellas, que requerirán un importante conocimiento técnico de su funcionamiento para prosperar”.



Paloma Llaneza: “Las compañías no cuentan con mayor incentivo para invertir en ciberseguridad que el riesgo reputacional y el judicial”

Para empezar, aunque la compañía afirmó inicialmente que usaba cifrado de extremo a extremo (E2E) para las reuniones de vídeo, más tarde se descubrió que en realidad utilizaba un cifrado TLS, que es el mismo tipo empleado para proteger sitios web HTTPS, no el E2E completo. La compañía también era vulnerable en las rutas UNC (Uniform Naming Convention), que permitían a los hackers capturar credenciales de inicio de sesión de Windows cuando los usuarios hacían clic en los enlaces. Los fallos también permitieron fugas de datos a Facebook, a intrusos, a compartir contenido inapropiado o perturbador durante las reuniones, y la venta de miles de cuentas en la dark web, que incluían direcciones de correo electrónico, contraseñas, URLs de reuniones y códigos de anfitrión.



Zoom no fue la única plataforma que no puso todo para minimizar los peligros de violaciones a la intimidad en sus sistemas. Webex, el servicio protagonista del escándalo en el Ejército alemán, sufrió intrusiones que permitieron a terceros ingresar a reuniones sin ser detectados, escuchar conversaciones privadas y acceder a datos confidenciales. Microsoft Teams, ampliamente utilizado por organizaciones y escuelas, ha tenido varios incidentes relacionados con la seguridad, entre los que se encuentran el uso de GIFs maliciosos para robar datos de los usuarios. A la lista se suman las videoconferencias a través de Google Meet, Jitsi Meet, Skype y la aplicación social HouseParty, que también se vieron comprometidas.

Todas atajaron muchos de esos **fallos con actualizaciones de seguridad y cambios en su política de privacidad**. La inclusión del cifrado, tanto el de tránsito (que protege los datos mientras se transmiten entre el dispositivo y el servidor), como el de extremo a extremo (que protege los datos en todo el recorrido, sin pasar por los servidores), ha sido crucial para proteger la privacidad en las videoconferencias.

Añadido a esto, se ofrecen varias configuraciones para mejorar la privacidad, como las salas de espera (permite que el anfitrión apruebe a los participantes antes de que se unan a la reunión), las contraseñas para reuniones (asegura que solo los invitados con la contraseña correcta puedan unirse) o el control de participantes (el anfitrión puede gestionar quién puede compartir pantalla, grabar la reunión, etc.).

Riesgos y beneficios de la IA

La más reciente implementación de la **inteligencia artificial (IA)** en las videollamadas ofrece muchos beneficios en términos de seguridad y funcionalidad, pero también plantea riesgos significativos para la privacidad. “La integración de la IA en este tipo de servicios puede ser un ejemplo de vector de ataque si la misma no se hace pensando en la privacidad y la seguridad por diseño y por defecto”, dijo Llanea. Las tecnologías de IA a menudo requieren grandes cantidades de datos para funcionar correctamente, lo que, en el contexto de las videollamadas, puede significar la recopilación de información sensible de audio, vídeo y texto. La IA va a analizar todo este contenido para mejorar la experiencia del usuario (por ejemplo, transcribirá automáticamente o traducirá en tiempo real). Pero este procesamiento afecta a datos personales, lo que puede implicar el uso no autorizado de esa información para personalizar publicidad o crear perfiles de comportamiento o vigilancia.

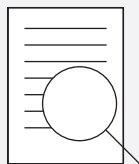
La IA va a analizar el contenido en tiempo real, lo que implica un procesamiento de datos personales que puede acarrear su uso no autorizado

Las herramientas de IA pueden ser utilizadas para monitorear continuamente las videollamadas, analizando expresiones faciales, tonos de voz y lenguaje corporal de los participantes. Pero lo que por un lado puede ser beneficioso para autenticar a los usuarios, puede resultar en una pérdida de anonimato y privacidad que facilite la usurpación de identidades, en caso de que esos datos biométricos queden expuestos. Incluso sobre la base del análisis de toda la información, **la IA podría interferir con la autonomía de los usuarios**: podría silenciarlos, expulsarlos o restringir ciertas acciones durante las videollamadas.

Además, las soluciones de IA a menudo operan de manera opaca, lo que dificulta a las personas entender cómo se usan sus datos y qué medidas de seguridad están implementadas. “La cuestión de mantenerlas seguras y, lo que es esencial, confidenciales, se debilita cuando estas herramientas se integran con otras, porque estos son puntos vulnerables en cualquier sistema” enfatizó.

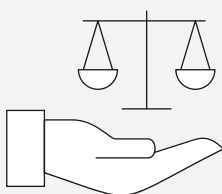
Por todo, los usuarios deben siempre tomar todas las **precauciones**. Deben revisar las políticas de privacidad de la plataforma que están utilizando, es decir, qué datos recopila la plataforma (información personal, datos de uso, grabaciones de las videoconferencias, etc.), cómo se usan esos elementos (si son para mejorar sus servicios, con fines de marketing o para compartir con terceros) y por cuánto tiempo se almacenan la información y cómo se pueden eliminar.

Además, es clave asegurarse de que la plataforma cumple con las regulaciones de privacidad aplicables, como el RGPD europeo. Regulaciones como esta exigen altos estándares de protección y ofrecen derechos a los usuarios sobre sus datos personales, lo que obliga a las empresas a actualizar constantemente sus políticas de privacidad y medidas de seguridad para cumplir con las normativas. La protección en las videoconferencias depende en gran medida de la tecnología utilizada, las directrices de la plataforma y las prácticas individuales. Elegir una plataforma fiable y configurarla correctamente es la mejor garantía posible para una mayor privacidad de las reuniones virtuales.

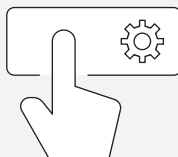


Revisa las políticas de privacidad:

- Datos que recopila
- Cómo los usa
- Por cuánto tiempo
- Cómo eliminarlos



Asegúrate de que cumple con las regulaciones de privacidad aplicables, como el RGPD europeo



Elige una plataforma fiable y configúrala correctamente



Sponsors



Colaboradores

