El caso Leonelli desde una perspectiva técnica:

El juez Andrés Leonelli fue investigado luego de que material sensible vinculado a una causa judicial terminara almacenado en la Nube. El sistema automático de Google detectó el contenido y generó un reporte internacional, lo que derivó en allanamientos e investigación penal. Posteriormente, la Justicia determinó que el material estaba relacionado con su trabajo judicial y que no existía delito. El caso abrió un fuerte debate sobre el manejo de información sensible en servicios de nube y los riesgos de utilizar entornos externos para custodiar evidencia o documentación crítica.
https://justierradelfuego.gov.ar/2025/09/12/la-justicia-penal-resolvio-que-el-juez-leonelli-no-cometio-un-delito

Más allá del resultado judicial, el caso dejó expuesto algo muchísimo más profundo:
Cómo están manejando los profesionales, la información sensible…
Vamos a analizarlo:

¿Qué ocurre cuando subimos algo a la nube?

La mayoría cree que subir un archivo es simplemente guardarlo en internet, en un lugar seguro.
Pero técnicamente ocurre mucho más que eso.
La realidad, es que ese archivo deja de existir solamente en tu dispositivo y pasa a almacenarse en **SERVIDORES EXTERNOS**.
Pero lo más importante no es solo dónde se guarda, sino lo que ocurre una vez que llega ahí.
La nube moderna no funciona como un simple depósito. Los sistemas procesan automáticamente la información: la indexan, la analizan, la replican, generan metadatos, calculan hashes y realizan escaneos de seguridad.
Dependiendo del servicio, también pueden detectar malware, reconocer imágenes, leer texto o identificar contenido sensible mediante inteligencia artificial y herramientas automatizadas.
Y todo esto ocurre incluso cuando la carpeta es **“PRIVADA”**.

¿Qué pasa cuando los sistemas identifican contenido ilegal?

Cuando el material sensible termina almacenado en la nube, los sistemas automáticos lo detectan mediante herramientas entrenadas para reconocer este tipo de contenido.
A partir de ahí, la plataforma actúa como fue diseñada:
bloquea la cuenta, genera alertas y activa toda la cadena de respuestas,

reportando el caso automáticamente a las autoridades para proceder a la investigación.

¿Pueden los sistemas entender la realidad detrás del archivo?

¡NO! ...La IA, el sistema o herramienta no entiende contexto, intención, funciones ni legitimidad..
No sabe si detrás de un archivo hay:
Un juez trabajando con evidencia, un médico analizando estudios, un perito investigando un delito o un criminal almacenando contenido ilegal o pornográfico…
Solo reconoce aquello para lo que fue entrenada y si detecta una coincidencia, actúa, reporta, bloquea y escala…Sin preguntarse absolutamente nada más!

¿las plataformas ven todo el contenido que subimos?

Es uno de los puntos más importantes y menos comprendidos
Cuando usamos estos servicios, aceptamos términos y condiciones que permiten a las plataformas aplicar procesos automáticos de seguridad sobre la información almacenada.
¿Para qué?..
Para detectar malware, spam, fraude, phishing, contenido ilegal, terrorismo y especialmente material de abuso infantil
Además, en muchos países, las empresas tecnológicas tienen obligaciones legales de reportar este tipo de contenido cuando es detectado por sus sistemas.
Por eso las plataformas, no ingresan y ven cada uno de los archivo que se carga, pero utilizan: hashes, herramientas, inteligencia artificial, machine learning y escaneos automáticos que analiza la información subida.

Y acá aparece algo clave:
Privado no significa que el sistema no pueda procesar la información.
Significa que otros usuarios no pueden acceder libremente a ella.
Pero la infraestructura del proveedor sí puede aplicar análisis automáticos por razones legales, técnicas y de seguridad.

Entonces… la nube ¿es SEGURA?

El problema muchas veces no es la nube en sí, sino cómo la ESTAMOS USANDO.
Cada vez más profesionales trabajan con datos críticos dentro de plataformas automatizadas que no operan con criterio humano… sino con patrones, estadísticas y reglas técnicas predefinidas.

Porque la nube moderna nos da comodidad, velocidad y acceso inmediato…
y eso es excelente!
en segundos… compartimos un archivo, lo abrimos desde el celular, seguimos trabajando desde la notebook, lo descargamos en casa, hacemos Backups automáticos
Y eso, objetivamente, es fantástico…

El verdadero problema aparece cuando esa misma comodidad nos hace olvidar algo fundamental:

Desde el momento en que cierta información entra en estos entornos, PERDEMOS EL CONTROL DEL MATERIAL.. que comienza a quedar sometido a políticas, sistemas y decisiones que nosotros NO CONTROLAMOS!

…AHÍ LA NUBE, DEJA DE SER UNA VENTAJA… PARA CONVERTIRSE EN UN RIESGO REAL PARA LA CUSTODIA, LA PRIVACIDAD Y LA INTEGRIDAD DE LA INFORMACIÓN SENSIBLE.!

Recomendaciones de seguridad para profesionales

- No usar nubes personales para información crítica
Los servicios de almacenamiento en la nube (cloud) son excelentes herramientas, muy cómodas y útiles, ideales para otros usos, pero no deberían ser el destino de expedientes, evidencia, informes o documentación sensible.

- Separar entornos
En lo posible, evitar mezclar trabajo sensible con dispositivos de uso cotidiano. La notebook personal no debería transformarse en repositorio de información crítica… al menos no, sin contar con medidas de seguridad mínimas y configuraciones adecuadas para proteger realmente esa información.

- Desactivar sincronización automática en carpetas sensibles
Escritorio, Documentos o Descargas muchas veces se sincronizan.
Y ahí, la información puede salir del entorno controlado sin que el usuario lo note.

- Saber exactamente dónde está cada archivo
Un profesional debería poder saber:
dónde está almacenada la información

quién tiene acceso
y si existe alguna copia o Backup automático.
NO se puede proteger lo que no se sabe dónde está guardado.

- Usar cifrado y almacenamiento offline
La información extremadamente sensible debe mantenerse fuera de línea y resguardada en entornos controlados y cifrados.

- Usar doble factor de autenticación (2FA)
En todas las cuentas.
No elimina todos los riesgos, pero agrega una capa crítica de protección y dificulta accesos indebidos, incluso cuando una contraseña fue comprometida.

- Tener políticas claras de manejo de información
Muchas filtraciones o incidentes no ocurren por ataques sofisticados, sino por hábitos improvisados.

- Capacitarse y asesorarse con personal especializado
Los mayores riesgos no aparecen por ataques sofisticados, sino por desconocer cómo funcionan realmente las herramientas que usamos todos los días.
Contar con capacitación y asesoramiento especializado permite tomar decisiones más seguras antes de que ocurra un incidente.

- Entender una regla básica:
La nube moderna es una infraestructura activa que analiza, procesa, clasifica, reporta y automatiza decisiones sobre la información que recibe.
La gran pregunta:
Si un sistema puede observar, interpretar y actuar sobre tus archivos…
¿es realmente privado?

El gran engaño, es hacernos creer que seguimos teniendo control absoluto, cuando ya lo perdimos….

Eduardo E. Lecce
Abogado
Ciberseguridad & Ethical Hacker
3624628578 - eelciberseguridad@gmail.com