#CHATCONTROL: EL FIN DE LA PRIVACIDAD EN INTERNET

Por: EL SUDAMERICANO. 26/07/2021

Todas tus conversaciones electrónicas (correos, mensajería electrónica) serán sospechosas y podrán ser intervenidas y enviadas a la policía

Hoy (6 de julio de 2021), el Parlamento Europeo aprobó **la Derogación de privacidad electrónica,** que **permite a los proveedores de servicios de correo electrónico y mensajería buscar automáticamente todos los mensajes personales de cada ciudadano en busca de contenido presuntamente sospechoso e informar los casos sospechosos a la policía.**

En la **votación de hoy** (6 de junio de 2021), 537 diputados al Parlamento Europeo aprobaron ***Chatcontrol***, con 133 votos en contra y 20 abstenciones.

Según datos policiales, en la gran mayoría de los casos, ciudadanos inocentes son sospechosos de haber cometido un delito debido a procesos poco fiables. En una encuesta representativa reciente, el 72% de los ciudadanos de la UE se opuso al seguimiento general de sus mensajes.

Si bien los proveedores inicialmente tendrán la opción de registrar o no las comunicaciones, la legislación de seguimiento, que se espera para el otoño, obligará a todos los proveedores de servicios de comunicaciones a realizar una selección indiscriminada.

La Comisión Europea ya ha anunciado un reglamento de seguimiento para que el Chat Control sea obligatorio para todos los proveedores de correo electrónico y mensajería. Los servicios de mensajería cifrados de extremo a extremo que antes eran “seguros”, como Whatsapp o Signal, se verían obligados a instalar una puerta trasera.

¿Pero qué es Chat Control?

La UE quiere que todos los chats, mensajes y correos electrónicos privados se

busquen automáticamente en busca de contenido sospechoso, de manera general e indiscriminada.

El objetivo declarado: perseguir la pornografía infantil. El resultado: vigilancia masiva a través de mensajería en tiempo real totalmente automatizada y control de chat y el fin del secreto de la correspondencia digital.

En 2020, la Comisión Europea propuso una legislación “temporal” destinada a permitir la búsqueda de todos los chats privados, mensajes y correos electrónicos en busca de representaciones ilegales de menores y el intento de inicio de contactos con menores.

Esto es para permitir a los proveedores de Facebook, Messenger, Gmail, etc., Escanear cada mensaje en busca de texto e imágenes sospechosas. Esto se lleva a cabo en un proceso totalmente automatizado y utilizando una “inteligencia artificial” propensa a errores.

Si un algoritmo considera que un mensaje es sospechoso, su contenido y metadatos se divulgan automáticamente y sin verificación humana a una organización privada con sede en EE. UU. Y de allí a las autoridades policiales nacionales de todo el mundo. No se notifica a los usuarios informados.

Algunos proveedores de servicios de EE. UU., Como Gmail y Outlook.com, ya están realizando dichos controles automatizados de mensajería y chat. Mediante una segunda ley, la Comisión de la UE tiene la intención de obligar a todos los proveedores de servicios de chat, mensajería y correo electrónico a implementar esta tecnología de vigilancia masiva.

¿Cómo nos afecta a todos?

- Todas sus conversaciones de chat y correos electrónicos se buscarán automáticamente en busca de contenido sospechoso. Nada permanece confidencial o secreto. No se requiere una orden judicial o una sospecha inicial para buscar sus mensajes. Ocurre siempre y automáticamente.
- Si un algoritmo clasifica el contenido de un mensaje como sospechoso, el personal y los contratistas de las corporaciones internacionales y las autoridades policiales pueden ver sus fotos privadas o íntimas. Además, sus fotos privadas de desnudos pueden ser vistas por personas que no conoce, en

cuyas manos sus fotos no están seguras.
- El personal y los contratistas de las corporaciones internacionales y las autoridades policiales pueden leer coqueteos y mensajes de texto sexuales, ya que los filtros de reconocimiento de texto que buscan “acicalamiento infantil” frecuentemente señalan falsamente las conversaciones íntimas.
- Puede ser denunciado e investigado falsamente por supuestamente difundir material sobre explotación sexual infantil. Se sabe que los algoritmos de mensajería y control de chat marcan fotos de vacaciones completamente legales de niños en una playa, por ejemplo.
- Según las autoridades de la policía federal suiza, el 86% de todos los informes generados por máquinas resultan sin fundamento. El 40% de todos los procedimientos de investigación penal iniciados en Alemania por “pornografía infantil” se dirigen a menores.
- En su próximo viaje al extranjero, puede esperar grandes problemas. Es posible que los informes generados por máquinas sobre sus comunicaciones se hayan transmitido a otros países, como EE. UU., Donde no hay privacidad de datos, con resultados incalculables.
- Los servicios de inteligencia y los piratas informáticos pueden espiar sus chats y correos electrónicos privados. La puerta estará abierta para que cualquier persona con los medios técnicos pueda leer sus mensajes si se elimina el cifrado seguro para poder filtrar los mensajes.
- Este es sólo el comienzo. Una vez que se ha establecido la tecnología para la mensajería y el control del chat, resulta muy fácil utilizarlos para otros fines. ¿Y quién garantiza que estas máquinas de incriminación no se utilizarán en el futuro en nuestros teléfonos inteligentes y portátiles?

Información y argumentos adicionales

- Todos los ciudadanos son puestos bajo sospecha, sin motivo, de posiblemente haber cometido un delito. Los filtros de texto y fotos monitorean todos los mensajes, sin excepción. No se requiere que ningún juez ordene tal monitoreo – a diferencia al mundo analógico que garantiza la privacidad de la correspondencia y la confidencialidad de las comunicaciones escritas. Según sentencia del Tribunal de Justicia de las Comunidades Europeas, el análisis automático permanente y generalizado de las comunicaciones privadas vulnera derechos fundamentales (caso C-511/18, párr. 192). Sin embargo, la UE ahora tiene la intención de adoptar dicha legislación. Para que la corte lo anule puede llevar años. Por lo tanto, debemos evitar la adopción de la legislación en primer

lugar.

- Se sacrifica la confidencialidad de la correspondencia electrónica privada. Los usuarios de los servicios de mensajería, chat y correo electrónico corren el riesgo de que se lean y analicen sus mensajes privados. Las fotos y el contenido de texto sensibles podrían enviarse a entidades desconocidas en todo el mundo y caer en las manos equivocadas. Según los informes, el personal de la NSA ha hecho circular fotos desnudas de ciudadanos y ciudadanas en el pasado. Se ha informado que un ingeniero de Google acecha a menores.
- La mensajería indiscriminada y el control del chat incrimina indebidamente a cientos de usuarios todos los días. Según la Policía Federal Suiza, el 90% del contenido informado por máquinas no es ilegal, por ejemplo, fotos inofensivas de vacaciones que muestran a niños desnudos jugando en la playa.
- La comunicación cifrada de forma segura está en riesgo. Hasta ahora, los algoritmos no pueden buscar mensajes cifrados. Para cambiar eso, las puertas traseras deberían estar integradas en el software de mensajería. Tan pronto como eso suceda, esta laguna de seguridad puede ser explotada por cualquier persona con los medios técnicos necesarios, por ejemplo, por los servicios de inteligencia extranjeros y los delincuentes. Se expondrían las comunicaciones privadas, los secretos comerciales y la información gubernamental confidencial. Se necesita un cifrado seguro para proteger a las minorías, las personas LGBTQI, los activistas democráticos, los periodistas, etc.
- Se está privatizando la justicia penal. En el futuro, los algoritmos de corporaciones como Facebook, Google y Microsoft decidirán qué usuario es sospechoso y cuál no. La legislación propuesta no contiene requisitos de transparencia para los algoritmos utilizados. En virtud del estado de derecho, la investigación de los delitos penales está en manos de jueces independientes y funcionarios públicos bajo la supervisión de los tribunales.
- La mensajería indiscriminada y el control del chat crean un precedente y abren las compuertas. Implementar tecnología para monitorear automáticamente todas las comunicaciones en línea es peligroso: se puede usar muy fácilmente para otros propósitos en el futuro, por ejemplo, violaciones de derechos de autor, abuso de drogas o “contenido dañino”. En estados autoritarios, esta tecnología sirve para identificar y arrestar a opositores al gobierno y activistas por la democracia. Una vez que la tecnología se implementa de manera integral, no hay vuelta atrás.
- La legislación temporal sobre la mesa es ineficaz. Contrariamente a su

intención, no permitirá que Facebook et al continúen con el monitoreo masivo de la correspondencia privada. Limita la directiva ePrivacy. Sin embargo, el control del chat continuará violando el Reglamento General de Protección de Datos (DSGVO) porque carece de base legal y viola el principio de proporcionalidad. La Agencia Irlandesa de Protección de Datos está examinando una denuncia presentada por Patrick Breyer.

LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ

Fotografía: Asociación de Internautas

Fecha de creación
2021/07/26