ONU alerta que privacidad en línea está más amenazada que nunca con programas espía

Un nuevo informe de la Oficina del Alto Comisionado de la ONU para los Derechos Humanos sobre la privacidad en la era digital advierte sobre las serias amenazas a las que se enfrenta el derecho a la intimidad de las personas por el uso cada vez más extenso de herramientas tecnológicas de vigilancia, control y opresión.

Debido a esta circunstancia, el estudio de ONU pide el control de estos medios cibernéticos mediante una regulación eficaz que cumpla con las leyes y las normas internacionales de derechos humanos.

El análisis se centra en tres áreas específicas: el abuso que cometen las autoridades estatales con las herramientas de piratería intrusiva (los programas espía, o spyware); el papel clave que desempeñan los métodos de encriptación en la protección de los derechos humanos en línea; y las repercusiones de la vigilancia digital generalizada de los espacios públicos, tanto en línea como fuera de internet, precisa una nota de prensa de la ONU divulgada este viernes 16.

«Las tecnologías digitales aportan enormes beneficios a las sociedades. Pero la vigilancia omnipresente tiene un alto coste, ya que socava los derechos y frena el desarrollo de democracias dinámicas y plurales», afirmó la Alta Comisionada en funciones para los Derechos Humanos de la ONU Nada Al-Nashif.

«En resumen, el derecho a la privacidad está más en peligro que nunca», subrayó y destacó que «por eso es necesario actuar y hacerlo ahora», dijo Nada Al-Nashif.

Los programas espía transforman nuestros teléfonos en dispositivos de vigilancia

En el primer caso, el informe de la ONU detalla cómo algunas herramientas de vigilancia –por ejemplo, el programa informático «Pegasus»–, pueden convertir la mayoría de los teléfonos inteligentes en «dispositivos de vigilancia las 24 horas del día», permitiendo al «intruso» acceder no solo a toda la información almacenada en nuestros móviles, sino que también los convierte en un arma para espiar nuestras vidas.

«Aunque supuestamente se despliegan para combatir el terrorismo

y la delincuencia, estas herramientas de espionaje se han utilizado a menudo por razones ilegítimas, como la represión de las opiniones críticas o disidentes y de quienes las expresan, incluidos los periodistas, las figuras políticas de la oposición y los defensores de los derechos humanos», afirma el informe.

Por ello, subraya la necesidad de tomar medidas urgentes para afrontar la propagación de los programas espía, y reitera el llamamiento a una moratoria sobre el uso y la venta de herramientas de piratería informática hasta que se establezcan las garantías adecuadas para la protección de los derechos humanos.

El informe sostiene que la intervención electrónica de un dispositivo personal por parte de las autoridades solo debería efectuarse como último recurso y en casos que sirvan «para prevenir o investigar un acto específico que suponga una amenaza grave para la seguridad nacional o un delito grave específico».

La encriptación de datos sigue debilitándose
Del mismo modo, considera que el cifrado de datos o encriptación representa un elemento clave para la privacidad y los derechos humanos en el ámbito digital, pero destaca que “se está socavando».

El estudio pide a los Estados que eviten tomar medidas que puedan restar eficacia al cifrado, como la instalación de las llamadas «puertas traseras», que permiten acceder a los datos cifrados personales o al control sistemático de los dispositivos de las personas.

Alerta ante el aumento de la vigilancia de los espacios públicos
El informe también alerta sobre la creciente vigilancia de los espacios públicos. Las limitaciones previas sobre el alcance de los métodos de observación quedaron destruidas por la recolección y el análisis automatizado de datos a gran escala, así como por los nuevos sistemas de identidad digitalizados y las extensas bases de datos biométricos que facilitan en gran medida la expansión de estas medidas de vigilancia.

Las nuevas tecnologías también han permitido la vigilancia sistemática de las opiniones que la gente expone en línea, incluida la recopilación y el análisis de las aportaciones de las redes sociales.

Además, se indica que a menudo los gobiernos no informan adecuadamente al público sobre sus actividades de vigilancia, e incluso que cuando se despliega este tipo de herramientas con

objetivos legítimos, pueden ser fácilmente reutilizadas, a menudo con fines para los que no estaban destinadas inicialmente.

El informe enfatiza que los Estados deben limitar las medidas de vigilancia pública a las «estrictamente necesarias y proporcionadas» y centradas en lugares y momentos concretos. Además, indica que debe limitarse la duración del almacenamiento de esos datos y que también es necesario restringir de inmediato el uso de sistemas de reconocimiento biométrico en espacios públicos.

Todos los Estados deben actuar también de inmediato para establecer regímenes sólidos de control de las exportaciones de tecnologías de vigilancia que plantean graves riesgos para los derechos humanos. Asimismo, deben asegurarse de que se lleven a cabo evaluaciones de impacto sobre los derechos humanos que tengan en cuenta de qué son capaces las tecnologías en cuestión, así como la situación en el país receptor.

EFE