DECLARACIÓN CONJUNTA DE LA SOCIEDAD CIVIL SOBRE EL USO DE SOFTWARE ESPÍA EN LA UNION EUROPEA Y MÁS ALLÁ

Somos una coalición de organizaciones de la sociedad civil y organizaciones de periodistas comprometidas con la protección de los derechos fundamentales, la transparencia y la rendición de cuentas en relación con las tecnologías de software espía. El software espía representa una seria amenaza contra los valores democráticos de la UE, el debate público y los espacios cívicos saludables, al socavar pilares críticos como la toma de decisiones independiente entre los legisladores y la capacidad de los periodistas y activistas para responsabilizar al poder. Además, como destacó el Supervisor Europeo de Protección de Datos, el nivel de intrusividad de las herramientas de software espía modernas vulnera la esencia del derecho fundamental a la privacidad y la protección de datos, lo que las hace ilegales según el derecho de la Unión.

El Comité de Investigación del Parlamento Europeo para investigar el uso de Pegasus y software espía de vigilancia equivalente (Comité PEGA) concluyó en mayo de 2023 que la mayoría de los Estados miembros de la UE habían comprado herramientas de software espía y que algunos de ellos han utilizado software espía para vigilar de manera ilegal y arbitraria a periodistas, defensores de los derechos humanos y políticos dentro de la UE, tal como han informado varias organizaciones de la sociedad civil.

Lamentamos profundamente que las Instituciones de la UE no hayan proporcionado soluciones efectivas ni un enfoque más completo ante los numerosos informes de mala administración y abuso de poder por parte de los Estados miembros durante la última legislatura.

Además, el recientemente adoptado Reglamento Europeo sobre la Libertad de los Medios de Comunicación (EMFA, por sus siglas en inglés) establece un precedente preocupante. A pesar de sus loables intenciones, la ley no protege completamente a los periodistas del software espía, careciendo de salvaguardas esenciales contra su vigilancia y creando bases legales demasiado amplias para su uso contra ellos en la UE. En consecuencia, tanto las víctimas de software espía como la sociedad de la UE en su conjunto continúan esperando una respuesta institucional adecuada a esta amenaza a los derechos fundamentales.

Las organizaciones firmantes creemos que el nuevo período legislativo ofrece una oportunidad para que las nuevas instituciones Europeas tomen medidas más decisivas e implementen el acervo comunitario de la UE en esta materia. La Comisión, el Consejo y el Parlamento deben tomar urgentemente medidas robustas para frenar el abuso del software espía en la UE y defender los valores Europeos respetando y protegiendo los derechos fundamentales, introduciendo mecanismos de rendición de cuentas efectivos y proporcionando recursos a las víctimas de la vigilancia ilegal con software espía. Además, los Estados miembros son responsables de salvaguardar los derechos fundamentales de todas las personas bajo su jurisdicción.

Instamos a las instituciones de la UE y a los Estados miembros a adoptar las siguientes medidas sin dilación:

Comisión Europea

- Proponer un nuevo marco legal de la UE que aborde los desafíos que plantea el software espía, que incluya una prohibición en toda la UE sobre la producción, exportación, venta, importación, adquisición, transferencia, mantenimiento y uso de software espía, que interfiera de manera desproporcionada con los derechos fundamentales y para el cual no existen salvaguardas adecuadas para prevenir y remediar los daños a los derechos humanos.

- Imponer una moratoria en la UE hasta que se establezca este nuevo marco legal.
- Impulsar la implementación de una prohibición completa sobre el desarrollo y la venta de software espía comercial por parte de empresas privadas.
- Asegurarse de que el marco legal existente se implemente adecuadamente por los Estados miembros, mediante la realización de una evaluación exhaustiva y profunda del cumplimiento por parte de los Estados miembros con las Directiva sobre la privacidad y las comunicaciones electrónicas, la Directiva sobre la protección de datos en el ámbito penal, así como con el Reglamento sobre productos de doble uso, y lanzar procedimientos de infracción contra aquellos Estados cuyo comercio y uso de software espía infrinja tales instrumentos.
- Fortalecer el régimen de control de exportaciones revisando y enmendando el Reglamento sobre productos de doble uso de la UE, especialmente al incorporar el software espía en la definición de herramientas de ciber-vigilancia e incluir obligaciones que garanticen que estas herramientas no se utilicen para la represión o violaciones de derechos humanos.
- Utilizar los instrumentos disponibles dentro del conjunto de herramientas al servicio del estado de derecho para supervisar el uso del software espía por parte de los Estados miembros. Esto incluye el despliegue del Marco del Estado de Derecho, incorporando hallazgos y conclusiones en el Informe Anual sobre el Estado de Derecho, iniciando procedimientos de infracción cuando sea necesario y aplicando el Régimen General de Condicionalidad para suspender los fondos de la UE en casos en los que el uso de software espía vulnere el estado de derecho y en caso de deficiencias en los mecanismos de control.
- Exigir transparencia en los contratos y operaciones gubernamentales de los Estados miembros de la UE relacionados con software espía, asegurando la rendición de cuentas en casos de abuso.
- Proponer una definición legal armonizada de seguridad nacional y establecer directrices para que los Estados miembros determinen una amenaza genuina y seria contra la seguridad nacional.
- Imponer una prohibición sobre la comercialización de vulnerabilidades para cualquier propósito que no sea el fortalecimiento de la seguridad de los sistemas y exigir la divulgación responsable de los hallazgos de investigaciones sobre vulnerabilidades.
- Asegurarse de que cualquier futura propuesta legislativa que potencialmente reemplace la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas proporcione mejores garantías para proteger la confidencialidad de las comunicaciones, en particular fortaleciendo el derecho a la protección de los equipos terminales ya garantizado por la Directiva de privacidad electrónica.

Consejo de la UE

- Abstenerse de introducir amplias excepciones de seguridad nacional en la legislación de la UE, ya que tales excepciones crean brechas significativas en la aplicabilidad y la ejecución de los instrumentos legales de la UE y exponen a los ciudadanos a más violaciones de derechos fundamentales.
- Organizar un debate sobre el uso de software espía dentro de la UE en el Consejo de Asuntos Generales y adoptar conclusiones relevantes.

Estados miembros de la UE

- Suspender todas las exportaciones fuera de la UE en la venta y transferencia de tecnología de vigilancia que hayan sido autorizadas en violación de las normas internacionales de derechos humanos.
- Abstenerse de incumplir sus obligaciones de derechos fundamentales bajo la Carta de Derechos Fundamentales de la UE y el Convenio Europeo de Derechos Humanos alegando excepciones por motivos de seguridad nacional.
- Imponer sanciones a los proveedores que se descubra que han infringido sus obligaciones de debida diligencia de acuerdo con el derecho de la UE.

- Comprometerse a mantener el nivel más alto o absoluto de protección a nivel nacional, evitando recurrir a la excepción contemplada en el Artículo 4, Párrafo 5, del Reglamento sobre la Libertad de los Medios de Comunicación que permite a los Estados miembros desplegar software de vigilancia intrusiva.

- Eliminar todos los obstáculos existentes que impiden a las víctimas de spyware acceder a la justicia y a los recursos adecuados, y asegurar que todas las investigaciones policiales y judiciales se gestionen de manera rápida, efectiva y transparente.

Parlamento de la UE

- Continuar con la investigación, el seguimiento y la propuesta de recomendaciones para reducir los abusos del spyware de vigilancia por parte de los Estados miembros, y seguir exigiendo la implementación completa de las recomendaciones del Comité PEGA.

- Utilizar todos los recursos a su disposición para ejercer sus poderes de escrutinio sobre la Comisión y el Consejo de la UE y para atribuir las responsabilidades pertinentes por su inacción, acciones insuficientes o incumplimiento de la legislación de la Unión existente

Enfatizamos que todos los dirigentes responsables de la toma de decisiones en relación con las recomendaciones mencionadas, sin excepción, deben consultar de manera pública y transparente con las partes interesadas nacionales e internacionales relevantes, incluidas las organizaciones de la sociedad civil, los grupos de derechos humanos y las entidades representativas de las víctimas de spyware.

Nosotros, las organizaciones firmantes, que representamos un colectivo de organizaciones de la sociedad civil y de periodistas, nos mantenemos unidas en la exigencia de una acción inmediata para respetar y proteger los derechos de todas las personas en la UE frente a la amenaza del spyware.

Members of the Coordination Group

Access Now
ARTICLE 19
Centre for Democracy & Technology Europe (CDT Europe)
Civil Liberties Union for Europe (Liberties)
Data Rights
Electronic Privacy Information Center (EPIC)
Epicenter.works - for digital rights
European Digital Rights (EDRi)
European Federation of Journalists (EFJ)
The Hungarian Civil Liberties Union (HCLU)
Privacy International (PI)
Wikimedia Europe

Additional signatories

Aspiration
Bulgarian Helsinki Committee
Digital Rights Ireland
Data Privacy Brasil
Centre for Peace Studies
Citizen D / Državljan D
Civil Rights Defenders
European Center for Not-for-Profit Law (ECNL)
Fundación Karisma (Colombia)
Homo Digitalis
Italian Coalition for Civil Liberties and Rights (CILD)
IT-Pol Denmark
Ligue des droits humains (Belgium)
Nederlands Juristen Comité voor de Mensenrechten (NJCM)
Panoptykon Foundation
Peace Institute (Slovenia)
Sflc.in (India)
Vrijschrift.org
Xnet, Institute for Democratic Digitalisation (Spain)