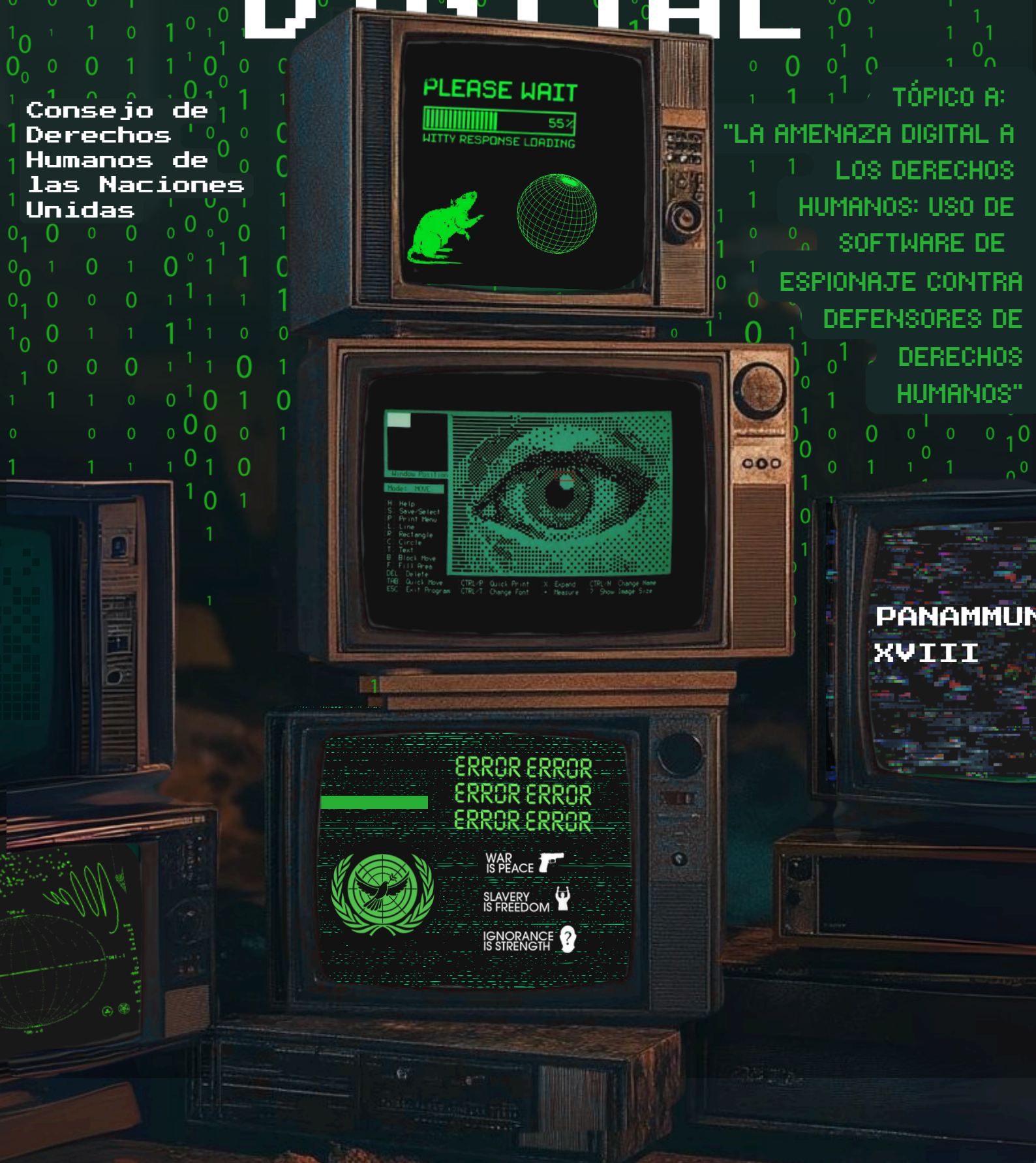
PRIVACIDAD DIGITAL

Consejo de Derechos Humanos de las Naciones Unidas

TÓPICO A:
"LA AMENAZA DIGITAL A LOS DERECHOS HUMANOS: USO DE SOFTWARE DE ESPIONAJE CONTRA DEFENSORES DE DERECHOS HUMANOS"



TÓPICO A. LA AMENAZA DIGITAL A LOS DERECHOS HUMANOS: USO DE SOFTWARE DE ESPIONAJE CONTRA DEFENSORES DE DERECHOS HUMANOS

"Desestimar la privacidad porque no tienes nada que ocultar es como descartar la libertad de expresión porque no tienes nada que decir".
- Edward Snowden

En la última década, el avance de las tecnologías digitales ha incrementado las capacidades de vigilancia de los Estados, especialmente a través de las interceptaciones digitales, también conocidas como espionaje digital, vigilancia electrónica o ciberespionaje. Estas prácticas consisten en el acceso remoto y encubierto a la información privada de las personas, incluyendo llamadas, mensajes, correos electrónicos, ubicación en tiempo real, fotografías e incluso en el control total de dispositivos electrónicos como teléfonos inteligentes, al activar cámaras y micrófonos sin que el usuario lo note.

Con el desarrollo de software avanzado, estas técnicas se han sofisticado, destacando el caso de Pegasus, creado por la empresa israelí NSO Group, que se ha convertido en el ejemplo más emblemático de *spyware*. Aunque originalmente diseñados para combatir amenazas graves como el terrorismo o el crimen organizado, la evidencia muestra que en muchos contextos estas herramientas se han empleado con fines políticos, de intimidación y persecución contra periodistas, activistas y personas defensoras de derechos humanos, lo que plantea un gran problema entre los límites de la seguridad nacional y la protección de los derechos fundamentales.

El auge de estas tecnologías en los últimos años es innegable. Según investigaciones de Citizen Lab y Amnistía Internacional, Pegasus ha sido detectada en más de 45 países y su uso se ha atribuido a gobiernos de todas las regiones del mundo. El software puede infiltrarse en dispositivos incluso a través de mensajes invisibles para el usuario, lo que lo convierte en una herramienta casi indetectable. Aunque NSO Group asegura que solo vende sus productos a Estados autorizados y con fines legítimos, múltiples informes han demostrado que han sido empleados para vigilar a críticos políticos, activistas y defensores de derechos humanos.

Uno de los ejemplos más documentados es el *Pegasus Project*, una investigación global de 2021 que reveló una lista de más de cincuenta mil números de teléfono seleccionados como posibles objetivos de espionaje. En esa lista aparecían periodistas, defensores, funcionarios e incluso jefes de Estado. Análisis forenses confirmaron que muchos de esos números efectivamente habían sido infectados.

En México, se documentaron al menos setenta y seis intentos de ataques contra periodistas y defensores de derechos humanos entre 2015 y 2016. Organizaciones como R3D, SocialTIC y Artículo 19, demostraron que los intentos de infección coincidían con periodos en los que esas personas publicaron investigaciones sensibles o denunciaron violaciones de derechos. Además, en 2017, se documentó que periodistas, activistas anticorrupción y defensores de víctimas de desapariciones forzadas fueron objeto de investigación, resultando en un espionaje digital ilegal. Entre los casos más emblemáticos se encuentran los de integrantes del Centro de Derechos Humanos Miguel Agustín Pro Juárez y de organizaciones de lucha contra la impunidad. Aunque el gobierno en turno justificó la adquisición del software como parte de su estrategia de seguridad, las pruebas señalaron que se usó contra actores sociales que representaban una voz crítica, debilitando la confianza en las instituciones. Investigaciones posteriores confirmaron que estas prácticas continuaron bajo nuevas administraciones.

En Colombia, la situación es igualmente preocupante. El Colectivo de Abogados “José Alvear Restrepo” (CAJAR) denunció durante décadas haber sido víctima de interceptaciones ilegales por parte de agencias estatales. En un contexto marcado por el conflicto armado, la vigilancia se dirigió contra defensores de derechos humanos, líderes sociales y opositores, generando un ambiente de intimidación. La llegada de tecnologías más sofisticadas intensificó este panorama. Informes recientes han señalado el posible uso de software avanzado de espionaje contra activistas en procesos de paz y en la defensa de comunidades afectadas por la violencia. En sociedades con debilidad institucional y altos niveles de conflictividad, la vigilancia digital puede convertirse en una herramienta de persecución política.

Este fenómeno no se limita a América Latina. En Hungría y Polonia, Pegasus fue utilizado para espiar a periodistas y miembros de la oposición política, lo que desató tensiones en la Unión Europea acerca de la compatibilidad de estas prácticas con los valores democráticos del bloque. En Marruecos, defensores de la causa Saharaui denunciaron haber sido vigilados mediante este software, en un contexto de represión a la libertad de expresión. En India, la Corte Suprema abrió una investigación en 2021 tras revelarse que líderes opositores, jueces y periodistas habían sido blanco de espionaje digital. En Arabia Saudita, las investigaciones sobre el asesinato del periodista Jamal Khashoggi revelaron que Pegasus pudo haber sido utilizado para vigilarlo a él y a su entorno cercano, lo que generó una fuerte condena internacional. En España, el espionaje a líderes independentistas catalanes en 2022 provocó un debate político interno y un cuestionamiento sobre el uso de estas tecnologías en sociedades democráticas.

El impacto de las interceptaciones digitales en los derechos humanos es profundo y multifacético. En primer lugar, se vulnera el derecho a la privacidad, reconocido en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Cuando la vigilancia se realiza sin orden judicial, sin proporcionalidad ni necesidad, se convierte en una violación directa de este derecho. En segundo lugar, la libertad de expresión se ve amenazada; periodistas y activistas sometidos a vigilancia pueden optar por la autocensura, debilitando la circulación de información y el debate público. En tercer lugar, se compromete la seguridad de defensores de derechos humanos, quienes enfrentan un entorno de hostigamiento e intimidación que limita su labor. Finalmente, la confianza en las instituciones se erosiona cuando los Estados recurren a prácticas opacas, generando una crisis de legitimidad democrática.

La comunidad internacional ha identificado dos enfoques principales frente a esta problemática. El primero de ellos radica en posiciones prohibicionistas, que sostienen que el potencial de abuso es tan alto que la única solución viable es la prohibición total de programas como Pegasus; el segundo, consta de algunos gobiernos que defienden un enfoque

regulacionista, argumentando que la vigilancia digital puede ser legítima si se limita a fines específicos y bajo estrictos controles judiciales de legalidad, necesidad y proporcionalidad.

El dilema no es menor. En contextos de amenazas reales, como el terrorismo internacional o las redes criminales transnacionales, la vigilancia digital puede salvar vidas. Sin embargo, cuando estas herramientas se utilizan para silenciar voces críticas, proteger intereses políticos o intimidar a la sociedad civil, la seguridad se convierte en un pretexto para restringir libertades. De ahí la necesidad de que los Estados entablen un diálogo multilateral abierto y transparente, que explore cómo diseñar marcos regulatorios que atiendan tanto las necesidades de seguridad como la protección de los derechos humanos.

La discusión no debe limitarse a los Estados. Las empresas que desarrollan y comercializan estos programas tienen también una responsabilidad ética y legal. Organismos internacionales han señalado que la falta de controles corporativos permite la venta de software a gobiernos con antecedentes de violaciones graves, lo que alimenta un mercado opaco. En este sentido, resulta fundamental promover estándares de debida diligencia empresarial, que obliguen a las compañías tecnológicas a garantizar que sus productos no se utilicen para violar derechos humanos.

Las interceptaciones digitales representan uno de los desafíos más urgentes para el sistema internacional de derechos humanos. La tecnología, lejos de ser neutral, puede convertirse en una herramienta de opresión si no se regula adecuadamente. La prohibición total parece inviable, mientras que la regulación exige un nivel de cooperación y transparencia que pocos Estados están dispuestos a asumir. Lo que está en juego es el equilibrio entre seguridad y libertad, un tema que va a delimitar la calidad de las democracias. El respeto de los derechos humanos sólo podrá alcanzarse mediante la voluntad política de proteger a quienes, con su labor, sostienen los principios de libertad y dignidad humana.

PREGUNTAS GUÍA:

- ¿Cómo han transformado las interceptaciones digitales la manera en que los Estados conciben la seguridad y el control social?
- ¿Qué derechos humanos se ven más comprometidos ante la vigilancia digital y de qué manera?
- ¿Cómo equilibrar el interés legítimo de los Estados en garantizar la seguridad con la obligación de proteger la privacidad y la libertad de expresión?
- ¿Qué enseñanzas dejan los casos de México y Colombia sobre los riesgos que enfrentan los defensores de derechos humanos ante el uso indebido de tecnologías de vigilancia?
- ¿Cómo influyen la debilidad institucional y la falta de transparencia en la proliferación de prácticas de espionaje digital indebido?
- ¿Qué medidas deben adoptar las empresas privadas desarrolladoras de spyware para garantizar que sus productos no se utilicen en violaciones de derechos humanos?
- ¿De qué manera las prácticas de interceptación digital afectan al trabajo de organizaciones de la sociedad civil y a la protección del espacio cívico?
- ¿Hasta qué punto la prohibición total de programas de interceptación es viable y efectiva para prevenir abusos?
- ¿Cómo puede el Consejo de Derechos Humanos promover estándares internacionales sobre legalidad, necesidad y proporcionalidad en el uso de estas tecnologías?

FUENTES DE CONSULTA:

- *Consejo de Derechos Humanos de las Naciones Unidas. Informe del Relator Especial sobre el derecho a la privacidad. A/HRC/46/37. (2021). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/043/13/PDF/G2104313.pdf*

- *Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. El impacto de la vigilancia digital en los derechos humanos. A/HRC/47/25. (2021). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/164/88/PDF/G2116488.pdf*

- *Asamblea General de la ONU. Declaración sobre los defensores de derechos humanos. A/RES/53/144. (1998). https://www.ohchr.org/es/instruments-mechanisms/instruments/declaration-human-rights-defenders*

- *Citizen Lab. Revisiting Pegasus: Technical report on surveillance in Mexico. (2017). https://citizenlab.ca/2017/06/revisiting-pegasus*

- *Amnistía Internacional. Uncovered: How Pegasus spyware was used against human rights defenders. (2021). https://www.amnesty.org/en/latest/research/2021/07/pegasus-project*

- *Comisión Interamericana de Derechos Humanos (CIDH). Situación de Defensores y Defensoras de Derechos Humanos en Colombia. (2019). http://www.oas.org/es/cidh/defensores/docs/pdf/defensores2019.pdf*

- *Parlamento Europeo. Report on the use of Pegasus and equivalent surveillance spyware. (2022). https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf*

- *Freedom House. Freedom on the Net 2023: Global Digital Rights Report. (2023). https://freedomhouse.org/report/freedom-net/2023*

- *Human Rights Watch. Digital Enemies: Surveillance Against Journalists and Activists. (2021).https://www.hrw.org/news/2021/12/21/global-surveillance-digital-enemies*

- *Organización de Estados Americanos (OEA). Resolución sobre protección de periodistas y defensores de derechos humanos en contextos de vigilancia digital. (2022). https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1202*

- *Relatoría Especial para la Libertad de Expresión de la CIDH. Informe Anual sobre Libertad de Expresión y Vigilancia Estatal. (2020). http://www.oas.org/es/cidh/expresion/informes/anuales.asp*

- *Reporteros Sin Fronteras (RSF). Predators of Press Freedom and Digital Surveillance. (2021). https://rsf.org/en/predators*
- *Naciones Unidas. Pacto Internacional de Derechos Civiles y Políticos. (1966) https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights*

- *Access Now. The Global Spyware Industry and Human Rights. (2022). https://www.accessnow.org/the-global-spyware-industry*

- *Relatoría Especial de la ONU sobre la libertad de opinión y expresión. Informe sobre vigilancia y derechos humanos. A/HRC/41/35. (2019). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/142/90/PDF/G1914290.pdf*