**CUESTIONARIO DE CONSULTA SOBRE TECNOLOGÍAS DE VIGILANCIA DIGITAL Y DERECHOS HUMANOS**

La Comisión Interamericana de Derechos Humanos (CIDH) y su Relatoría Especial para la Libertad de Expresión (RELE) han identificado desafíos en la región con relación al uso estatal de tecnologías de vigilancia digital y su supervisión; el papel del mercado privado en el desarrollo, mantenimiento y proliferación de dichas tecnologías; y la falta de rendición de cuentas por los abusos contra los derechos humanos facilitados por dichas tecnologías. Tras años de investigación e información sobre los abusos de la vigilancia, y el reconocimiento abrumador por parte de la comunidad internacional de los riesgos que las tecnologías de vigilancia suponen para los derechos humanos, la seguridad nacional y la propia democracia, se ha logrado poco progreso en una reforma sistémica genuina. En particular, las personas que saben o sospechan que están siendo vigiladas en violación de sus derechos siguen careciendo de recursos o remedios efectivos para enfrentarse a los aparatos de seguridad estatal y a las entidades del sector privado que los abastecen.

En este contexto, la Relatoría Especial preparará un informe temático centrado en el uso de las tecnologías de vigilancia digital en las Américas, destacando su impacto sobre el derecho a la libertad de expresión, la libertad de prensa y los derechos humanos y el Estado de derecho en general. El informe evaluará los efectos acumulativos y las implicaciones de los abusos de vigilancia documentados en los últimos años en la región, incluyendo las percepciones y prácticas de las autoridades estatales, el sector privado y la sociedad civil en lo que se ha convertido en una relación invertida entre los medios cada vez más amplios de vigilancia digital intrusiva y los derechos a la libertad de expresión y a la privacidad. El informe examinará los impedimentos existentes para la transparencia, la reparación y la no repetición del uso indebido. Explorará las mejores prácticas para establecer una supervisión y una rendición de cuentas pública en la vigilancia digital que hagan efectivos los derechos implicados, restauren la confianza pública en su protección y prevengan nuevos abusos. El informe avanzará en el desarrollo de estándares interamericanos y formulará recomendaciones a los Estados y al sector privado para hacer frente a estos retos.

La Relatoría Especial invita a los Estados, organizaciones de la sociedad civil, periodistas y medios de comunicación, defensores de derechos humanos, investigadores e instituciones académicas y otras personas interesadas a presentar la información que consideren pertinente sobre el tema, en particular sobre los aspectos señalados en el Cuestionario anexo.

**Plazo para responder:** 30 de agosto de 2024.

**Enviar a:** CIDHexpresion@oas.org

**Formato:** Español, inglés, francés o portugués. Respuestas concisas y objetivas con fuentes verificables. Puede responderse total o parcialmente. Además, se pueden adjuntar otros materiales de apoyo a la presentación, como informes, estudios académicos y otros tipos de materiales de referencia ya preparados y/o publicados que sean relevantes para el tema.

La Relatoría Especial para la Libertad de Expresión es una oficina creada por la Comisión Interamericana de Derechos Humanos (CIDH) para impulsar la defensa hemisférica del derecho a la libertad de pensamiento y expresión, considerando su papel fundamental en la consolidación y desarrollo del sistema democrático**.**

**Cuestionario de consulta**

La Oficina del Relator Especial agradece recibir información sobre lo siguiente:

1. *Incidentes de uso indebido.* Sírvase proporcionar los siguientes detalles concisos sobre incidentes verificados o presuntos de uso indebido por parte de las autoridades estatales de las tecnologías de vigilancia digital ocurridos en los Estados de la OEA:
	1. Individuo(s), comunidad(es) o entidad(es) destinataria(s).
	2. Tipo de tecnología de vigilancia digital empleada.
	3. Identidad del operador de la tecnología de vigilancia, desarrollador, intermediarios u otras entidades estatales o privadas clave asociadas con el incidente, si se conoce.
	4. ¿Se han tomado medidas legales, administrativas o de otro tipo para remediar el incidente? En caso afirmativo, ¿cuál es la situación actual?
	5. ¿Se obtuvo una reparación (por ejemplo, compensación económica, garantías de no repetición, etc.)?
	6. ¿Se determinó qué datos concretos se controlaron o se extrajeron del dispositivo? En caso afirmativo, ¿fue esta información facilitada por las autoridades estatales o a través de una investigación independiente?
	7. ¿Se inició algún tipo de violencia, represalia o vigilancia ilegal adicional contra la persona o entidad tras el incidente original?
	8. Enlaces a cualquier documentación justificativa.
2. *Políticas, leyes y reglamentos de los Estados relativos al uso de tecnologías de vigilancia digital*.
	1. ¿Qué autoridades estatales están autorizadas a llevar a cabo actividades de vigilancia digital y en virtud de qué leyes y reglamentos específicos?
	2. ¿Qué leyes o políticas, si las hay, establecen límites con respecto a la naturaleza, el alcance y la duración de las medidas de vigilancia empleadas por las autoridades estatales; las razones para ordenarlas; las autoridades con poder para autorizarlas, ejecutarlas y supervisarlas; y los mecanismos legales por los que pueden ser impugnadas?
	3. ¿Qué leyes o políticas especifican los criterios que deben utilizarse para determinar los casos en los que la vigilancia digital es legítima?
	4. ¿Qué procedimientos de supervisión ex ante y ex post existen para el uso de técnicas de vigilancia digital? ¿Existen órganos de supervisión independientes que controlen las actividades de vigilancia digital del Estado? ¿Qué garantías procesales se ofrecen?
	5. ¿Hace pública el Estado información relativa al marco regulador de los programas de vigilancia; las entidades encargadas de su aplicación y supervisión; los procedimientos de autorización, elección de objetivos y utilización de los datos recopilados; y el uso de estas técnicas, incluida información agregada sobre su alcance?
	6. ¿En qué Estados existen políticas y procesos específicos para el almacenamiento gubernamental frente a la divulgación de vulnerabilidades digitales (por ejemplo, procesos de equidad de vulnerabilidades [VEP])? Indique el contenido de dichas políticas y la composición de los órganos decisorios pertinentes. ¿Publica el Estado información sobre los resultados de dichos procesos?
	7. ¿De qué recursos disponen los Estados de la OEA para las personas sometidas a abusos de vigilancia digital? Especifique las leyes aplicables, las causas de acción pertinentes, los recursos administrativos, etc.
	8. ¿Qué postura han adoptado los Estados respecto a los *Principios de Tshwane sobre Seguridad Nacional y Derecho a la Información*?
	9. ¿Han promulgado los Estados algún requisito relativo a la notificación de las personas objeto de vigilancia digital?
	10. ¿Cómo han investigado los Estados los incidentes de vigilancia denunciados? ¿Cuáles han sido los resultados de dichas investigaciones?
	11. ¿Cómo han abordado las autoridades de protección del consumidor o de privacidad de datos de los Estados de la OEA el uso indebido de las tecnologías de vigilancia digital?
3. *El alcance del mercado privado de tecnologías de vigilancia digital en la región*.
	1. ¿Qué empresas de vigilancia digital operan en la región? ¿Quiénes son sus inversores y propietarios? ¿Mantienen sedes u operaciones en la región? ¿Han contratado personal en la región?
	2. Dentro de los Estados de la OEA, ¿qué entidades comerciales han operado dentro de la cadena de suministro de tecnologías de vigilancia digital? ¿Qué normas se aplican, en su caso, a los intermediarios u otros elementos de esta cadena de suministro?
	3. Entre los Estados de la OEA, ¿qué requisitos de registro, información u otro tipo de transparencia existen para las empresas que operan en el mercado de las tecnologías de vigilancia digital (incluidos desarrolladores, intermediarios, inversores, etc.)?
	4. ¿Qué legislación o normativa de los Estados de la OEA regula el desarrollo por parte de empresas privadas (en todas sus fases, incluidas las pruebas) de herramientas de vigilancia digital? ¿Se aplica alguna limitación al desarrollo de dichas herramientas por parte del sector privado?
	5. ¿Qué restricciones, si las hay, se aplican a la propiedad intelectual desarrollada o propiedad de empresas comerciales de software espía? ¿Poseen o han reclamado los Estados algún derecho de propiedad intelectual sobre las tecnologías de vigilancia digital adquiridas por entidades estatales, o que desarrollan las empresas que operan dentro de sus jurisdicciones?
	6. ¿Qué controles de exportación se aplican a las empresas que operan en el mercado de las tecnologías de vigilancia digital? ¿Qué sanciones, en su caso, se han aplicado a dichas empresas?
	7. ¿Qué políticas de adquisición y restricciones mantienen los Estados con respecto al mercado de la tecnología de vigilancia digital?
	8. ¿Han establecido los Estados alguna restricción a la inversión en empresas que formen parte del mercado de las tecnologías de vigilancia digital?
4. *Transparencia, responsabilidad y recurso*.
	1. ¿Cuáles son los principales retos a la hora de solicitar reparación por abusos de vigilancia verificados o presuntos?
	2. ¿De qué fuentes de pruebas se dispone para determinar la ilegalidad de la selección de objetivos mediante tecnologías de vigilancia digital?
	3. ¿Han sido las solicitudes de libertad de información un medio útil para obtener información sobre los abusos de la vigilancia digital?
	4. ¿Han prestado las fuerzas del orden u otros organismos estatales algún tipo de asistencia a personas o entidades sometidas a vigilancia digital ilegal?
	5. ¿Han iniciado las autoridades estatales procedimientos penales contra los presuntos autores y, en caso afirmativo, cuál ha sido el resultado?
	6. ¿Es viable la vía civil? ¿De qué causas nacionales disponen las personas víctimas de violaciones de sus derechos humanos reconocidos internacionalmente? ¿Qué obstáculos concretos se encuentran a la hora de emprender acciones legales?
	7. ¿Las personas o entidades que han sacado a la luz actividades ilegales de vigilancia digital han sufrido algún tipo de represalia por parte de los Estados o del sector privado?
	8. ¿Han obtenido los afectados algún tipo de reparación con respecto a un incidente de abuso de vigilancia? En caso afirmativo, describa el proceso por el que se obtuvo dicha reparación.
	9. ¿Han obtenido las personas o entidades sometidas a vigilancia digital sancionada por el Estado información relativa a los datos personales recopilados como resultado de dicha vigilancia?
	10. ¿Han obtenido garantías de no repetición las personas o entidades sometidas a vigilancia digital sancionada por el Estado?
5. *Lagunas, buenas prácticas y recomendaciones*.
	1. ¿Qué cambios jurídicos o políticos se han introducido en los Estados Miembros de la OEA en respuesta a los continuos informes sobre el uso indebido de las tecnologías de vigilancia digital?
	2. ¿Qué tendencias jurídicas, políticas o normativas cree que están cristalizando en este ámbito?
	3. ¿Cuál ha sido el impacto de la vigilancia digital sobre el derecho a la libertad de expresión en la región? ¿Han experimentado la sociedad civil, los medios de comunicación y/o el público en general efectos amedrentadores?
	4. ¿Qué papel desempeñan las tecnologías de vigilancia digital en la represión transnacional? ¿Qué buenas prácticas podrían contribuir a frenar la persecución extraterritorial?
	5. ¿Es necesaria una nueva legislación para abrir vías de recurso viables a las personas y entidades afectadas por los abusos de la vigilancia digital?
	6. ¿Qué formas de apoyo son más útiles para la sociedad civil, los periodistas y otras personas objeto de las tecnologías de vigilancia digital?
	7. ¿Cuáles son las mejores prácticas para notificar a las personas objeto de tecnologías de vigilancia digital?
	8. ¿Cuáles son las mejores prácticas, por parte de los Estados y del sector privado, para garantizar la transparencia en torno a la proliferación y el uso de las tecnologías de vigilancia digital?
	9. ¿Cuáles son las mejores prácticas para supervisar el uso de las tecnologías de vigilancia digital? ¿Qué papel deben desempeñar las autoridades judiciales?
	10. ¿Qué formas de desarrollo de capacidades serán esenciales para promover la supervisión y la rendición de cuentas en relación con la proliferación y el uso de las tecnologías de vigilancia digital?
	11. ¿Qué características técnicas de las herramientas de vigilancia digital podrían adaptarse para facilitar de forma fiable la transparencia, la supervisión y la responsabilidad en el uso?
6. ¿Desea añadir alguna información o comentario adicional sobre el tema de este cuestionario?