



HACIA UNA MORATORIA MUNDIAL DE LA TECNOLOGÍA DE VIGILANCIA SELECTIVA

INTRODUCCIÓN

Los ataques digitales contra defensores y defensoras de los derechos humanos, periodistas y la sociedad civil van en aumento. Cada vez hay más pruebas de que gobiernos y empresas violan los derechos humanos de activistas, periodistas y profesionales de la abogacía, entre otras personas, al someterlas a vigilancia selectiva ilegítima. Demasiados Estados de todo el mundo han hecho oídos sordos y permitido la exportación de tecnología de vigilancia a gobiernos que tienen un historial de uso de programas espía para violar los derechos humanos. No se pueden seguir ignorando esas violaciones de derechos humanos.

La idea de una moratoria a las exportaciones de tecnología de vigilancia cobró prominencia mundial por primera vez cuando, en su informe de 2019, el ex relator especial sobre la libertad de expresión David Kaye formuló la siguiente recomendación: “Los Estados deben imponer una moratoria inmediata a la exportación, venta, transferencia, uso o prestación de servicios de asistencia para instrumentos de vigilancia desarrollados por empresas privadas hasta que se establezca un régimen de salvaguardias que respete los derechos humanos”.¹ Desde entonces, Estados,² personas expertas en derechos humanos³ y numerosos actores de la sociedad civil han hecho suya esta petición.

¿QUÉ ES LA VIGILANCIA SELECTIVA ILEGÍTIMA?

La vigilancia selectiva ilegítima tiene dos dimensiones principales. La primera se da cuando se somete a vigilancia a personas por ejercer sus derechos humanos, o, de forma discriminatoria, por su identidad. Hay numerosos ejemplos de este tipo de casos, como la vigilancia de periodistas por informar sobre cuestiones desde una perspectiva crítica con un gobierno, de activistas por organizar protestas, o de personas de una etnia, raza, orientación sexual o religión determinadas por considerarlas delincuentes o posibles delincuentes.

Someter a la gente a vigilancia sobre esa base no se ajusta en ningún caso al derecho de los derechos humanos.

La segunda dimensión de la vigilancia selectiva ilegítima abarca los casos en los que la vigilancia puede tener alguna base legítima —como cuando se sospecha razonablemente que una persona ha cometido un delito— pero el sistema que posibilita esa vigilancia puede ser ilegítimo si no ofrece las salvaguardias adecuadas (incluido el recurso) contra los abusos.

Una de las razones más importantes por las que esto es así tiene que ver con el concepto de “efecto disuasorio”, que en este contexto se refiere al fenómeno por el cual la gente se abstiene de ejercer sus derechos por miedo a ser sometida a vigilancia. En otras palabras, “[i]ncluso la mera posibilidad de que pueda captarse información de

¹ Informe del relator especial, David Kaye, A/HRC/41/35 (2019), párr. 66.

² <https://www.accessnow.org/costa-rica-primer-pais-moratoria-spyware/>

³ *Spyware Scandal: UN experts call for moratorium on sale of 'life-threatening' surveillance tech*, 12 de agosto de 2021, <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379>

las comunicaciones crea una injerencia en la vida privada y puede tener un efecto negativo en derechos como los relativos a la libertad de expresión y de asociación.”⁴

La investigación corrobora que es menos probable que los activistas que temen estar sometidos a vigilancia — incluso sin tener pruebas de ello— estén dispuestos a expresar opiniones críticas sobre el gobierno, organizar protestas, reunirse libremente con colegas, o incluso hablar por teléfono o enviar mensajes de correo electrónico, por no saber de qué manera se podrán usar contra ellos en el futuro esas actividades.⁵

Este tipo de autocensura surge cuando los Estados no establecen las salvaguardias adecuadas, de modo que puede resultar imposible saber quién está sometido a vigilancia, cómo y por qué. En este tipo de casos, “no se puede decir que la sospecha y la preocupación generalizadas entre la población de que se está abusando de las facultades de vigilancia secreta sean injustificadas [...]. En estas circunstancias, hay base para alegar que la propia amenaza de vigilancia restringe la libre comunicación mediante los servicios de correos y telecomunicaciones y, por lo tanto, constituye para todos los usuarios reales y potenciales una interferencia directa con el derecho [a la vida privada y familiar].”⁶

En otras palabras, el hecho de que las salvaguardias sean inadecuadas no sólo afecta a los derechos de las personas sometidas a vigilancia, sino a los de todas las personas.

UNA MORATORIA COMO REFUERZO A LOS DERECHOS

Aunque las investigaciones realizadas por organizaciones de la sociedad civil y de medios de comunicación han demostrado que ambos tipos de vigilancia selectiva ilegítima existen a gran escala, también está claro que la vigilancia selectiva ilegítima debida a la falta de salvaguardias es casi universal. Como el relator especial David Kaye lo resumió, “[d]ecir que todo un sistema completo de control y utilización de tecnologías de vigilancia selectiva ha dejado de funcionar ni siquiera se acerca a la realidad. La realidad es que apenas existe”.⁷ Sin una moratoria inmediata, el uso ilegítimo de tecnología de vigilancia seguirá teniendo efectos devastadores en los derechos humanos no sólo de las personas a las que se somete a ella, sino de todas las personas.

Una moratoria sobre los programas espía tiene dos objetivos principales: 1) detener la venta, la transferencia y el uso de programas espía, pero también, y de manera crucial, 2) reforzar las salvaguardias de derechos humanos.

A la luz de esto, tal vez la forma más adecuada de concebir una moratoria consista en fortalecer el derecho a la privacidad (y a otros derechos asociados que se ven afectados por la vigilancia ilegítima). En efecto, una moratoria es una reafirmación de la prohibición existente de la vigilancia ilegítima, y un refuerzo de los derechos humanos.

POSIBLES MODELOS

Una moratoria sobre los programas espía tendría que ser una lista de salvaguardias de derechos humanos que los Estados debiesen poner en práctica para ser autorizados a vender, transferir o usar tecnología de vigilancia selectiva.

⁴ Alto comisionado de las Naciones Unidas para los derechos humanos, *El derecho a la privacidad en la era digital*, A/HRC/27/37, 30 de junio de 2014, párr. 20.

⁵ Amnistía Internacional, “Basta con que la gente crea que existe”: *Sociedad civil, secretismo y vigilancia en Bielorrusia*, EUR 49/4306/2016, <https://www.amnesty.org/es/documents/eur49/4306/2016/es/>

⁶ *Roman Zakharov v. Russia*, Tribunal Europeo de Derechos Humanos, párr. 171.

⁷ Informe del relator especial, David Kaye, A/HRC/41/35 (2019), párr. 46.

El derecho internacional de los derechos humanos ofrece numerosos ejemplos de cómo hacerlo. Por ejemplo, el Tratado sobre el Comercio de Armas⁸ o los tratados propuestos para regular los sistemas robóticos autónomos letales (denominados “robots asesinos”)⁹ o sobre el comercio de “instrumentos de tortura”¹⁰ ofrecen criterios según los cuales los Estados deben establecer salvaguardias relativas a los instrumentos o la tecnología que se prestan tanto a usos legítimos como ilegítimos a fin de ofrecer garantías frente a los abusos derivados de su fabricación, uso o transferencia.

CONCLUSIÓN

La necesidad de una moratoria mundial de la venta, transferencia y uso de la tecnología de vigilancia selectiva es clara y urgente. La venta y el uso no regulados y opacos de estos productos implican que puede que nunca conozcamos la verdadera magnitud de abusos similares en los que estén implicados otros actores. El mundo debe dejar de hacer caso omiso a esta enorme amenaza mundial para nuestros derechos.

¿Preguntas o comentarios? Contacto: rebecca.white@amnesty.org

⁸ Tratado sobre el Comercio de Armas, aprobado el 2 de abril de 2013, A/RES/ 67/234B, vigente desde el 14 de diciembre de 2014, art. 7.

⁹ Human Rights Watch, *New Weapons, Proven Precedent: Elements of and Models for a Treaty on Killer Robots*, octubre de 2020, <https://www.hrw.org/report/2020/10/20/new-weapons-proven-precedent/elements-and-models-treaty-killer-robots>

¹⁰ Amnistía Internacional, *Poner fin al comercio de la tortura: El camino hacia controles mundiales sobre los “instrumentos de tortura”*, <https://www.amnesty.org/es/documents/act30/3363/2020/es/>