Naciones Unidas A/HRC/41/35

Asamblea General

Distr. general
28 de mayo de 2019
Español
Original: inglés

Consejo de Derechos Humanos
41er período de sesiones
24 de junio a 12 de julio de 2019
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

La vigilancia y los derechos humanos

Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*

Resumen

La vigilancia de algunas personas —a menudo periodistas, activistas, personalidades de la oposición, críticos y otras personas que ejercían su derecho a la libertad de expresión— ha conducido en ocasiones a la detención arbitraria, a veces a la tortura y tal vez a ejecuciones extrajudiciales. Esas actividades de vigilancia han prosperado en medio de la debilidad de los controles sobre la exportación y la transferencia de tecnología a gobiernos con políticas de represión conocidas. En el presente informe, el Relator Especial comienza por definir el problema de la vigilancia selectiva desde la perspectiva de las obligaciones que el derecho de los derechos humanos impone a los Estados y las responsabilidades conexas que incumben a las empresas. A continuación, propone un marco jurídico y de políticas para la regulación, la rendición de cuentas y la transparencia en el sector de la vigilancia privada. El Relator Especial concluye con un llamamiento a la imposición de una regulación más rigurosa de las exportaciones de equipos de vigilancia y unas restricciones más estrictas de su utilización, así como de una moratoria inmediata sobre la venta y la transferencia a nivel mundial de los instrumentos que utiliza el sector de la vigilancia privada hasta que se establezcan estrictas salvaguardias de los derechos humanos en la regulación de esas prácticas y se pueda garantizar que los gobiernos y los agentes no estatales van a utilizar esos instrumentos de un modo legítimo.

* Este informe se presenta con retraso para poder incluir en él la información más reciente.

GE.19-08652 (S) 180619 190619
1908652

Índice

		Página
I.	Introducción	3
II.	Los gobiernos y el sector de la vigilancia privada	3
III.	Marco jurídico	8
IV.	Marco para la protección de los derechos fundamentales contra la vigilancia selectiva	15
V.	Recomendaciones	22

I. Introducción

1. La Asamblea General ha condenado la vigilancia y la interceptación ilícitas o arbitrarias de las comunicaciones como “actos graves de intrusión” que interfieren con los derechos humanos fundamentales (véanse las resoluciones de la Asamblea General 68/167 y 71/199). Sin embargo, las actividades ilegales de vigilancia se siguen llevando a cabo, al parecer sin dificultades. En las comunicaciones recibidas con ocasión de la redacción del presente informe se detallan, uno tras otro, casos de gobiernos que utilizan programas informáticos de vigilancia desarrollados, comercializados y mantenidos por empresas privadas. La vigilancia de personas concretas —a menudo periodistas, activistas, personalidades de la oposición, críticos y otras personas que ejercían su derecho a la libertad de expresión— ha conducido en ocasiones a la detención arbitraria, a veces a la tortura y tal vez a ejecuciones extrajudiciales. Esas actividades de vigilancia han prosperado en medio de la debilidad de los controles sobre la transferencia de tecnología a gobiernos con políticas de represión conocidas. Ese mercado está envuelto en un velo de secretismo; de hecho, nuestro conocimiento del problema se debe principalmente al trabajo forense en el terreno digital de investigadores no gubernamentales, y a labor tenaz de denuncia por parte de las organizaciones de la sociedad civil y los medios de comunicación.

2. El problema es tan grave como para que el Relator Especial concluya el presente informe de con un llamamiento no solo a la imposición de una regulación más rigurosa de las exportaciones de equipos de vigilancia y unas restricciones más estrictas de su utilización, sino de una moratoria inmediata sobre la venta y la transferencia a nivel mundial de los instrumentos que utiliza el sector de la vigilancia privada hasta que se establezcan estrictas salvaguardias de los derechos humanos en la regulación de esas prácticas y se pueda garantizar que los gobiernos y los agentes no estatales van a utilizar esos instrumentos de un modo legítimo.

3. El Relator Especial propone un marco jurídico y de políticas para la regulación, la rendición de cuentas y la transparencia en el sector de la vigilancia privada. Comienza por definir el problema, poniendo de relieve su especial atención a la vigilancia selectiva, dejando de lado la cuestión de la interceptación, recopilación y conservación de grandes volúmenes de información privada (denominada a menudo “vigilancia en masa”). A continuación, destaca las obligaciones que el derecho de los derechos humanos impone a los Estados y las responsabilidades conexas que incumben a las empresas. En la parte IV, propone un marco para mejorar las leyes y políticas existentes mediante la incorporación de la protección del derecho a la libertad de opinión y de expresión, sobre la base de las normas internacionales vigentes en la esfera de los derechos humanos. Concluye formulando recomendaciones para los principales interesados.

4. Para la preparación del presente informe se contó con la aportación de información contenida en 11 comunicaciones de los Estados y 33 de la sociedad civil. La Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH) organizó una consulta con expertos de dos días de duración en Bangkok en diciembre de 2018. Las comunicaciones recibidas y las conversaciones celebradas durante la consulta se resumen en una adición al presente informe[1].

II. Los gobiernos y el sector de la vigilancia privada

5. Vivimos en una era en la que abundan dispositivos para la vigilancia digital que son difíciles de detectar y que se prestan al uso abusivo. En su histórico informe sobre la vigilancia realizado en 2013, el anterior titular del mandato, Sr. Frank La Rue, señaló que la debilidad de los marcos normativos había proporcionado un terreno fértil para la vulneración ilícita y arbitraria del derecho a la intimidad y de la libertad de opinión y de

[1] Deseo expresar un especial agradecimiento a Amos Toh, Desiree Murray, Cristina Butoiu, Matthew Marcoly y Kyoolee Park, de la International Justice Clinic, en la Facultad de Derecho de Irvine de la Universidad de California, por su asistencia en la preparación del presente informe y su adición.

expresión (A/HRC/23/40, párr. 3). En el informe inaugural del Alto Comisionado para los Derechos Humanos, sobre la privacidad en la era digital, que se presentó el año siguiente, se llegaba a la conclusión de que las prácticas de muchos Estados habían puesto de manifiesto la ausencia de leyes nacionales adecuadas o de falta de rigor en su aplicación, la escasez de garantías procesales y la ineficacia de la capacidad de supervisión, elementos que habían contribuido a que no hubiese que rendir cuentas por las actividades ilícitas de vigilancia digital (A/HRC/27/37, párr. 47).

6. Algunos Estados desarrollan instrumentos para la vigilancia selectiva dentro de sus propios organismos y departamentos, otros dan un nuevo uso a los productos habituales de lucha contra la delincuencia y otros pueden adquirir sofisticados programas de espionaje en el mercado internacional de productos de vigilancia[2]. En el presente informe, el Relator Especial se ocupa sobre todo de esa última categoría de elementos. La vigilancia digital ya no está reservada a los países que disponen de los recursos necesarios para llevar a cabo una vigilancia en masa o selectiva mediante instrumentos elaborados a nivel interno. El sector privado ha entrado en escena, sin supervisión y con una forma de actuar muy cercana a la impunidad. Según Privacy International, en 2016 había más de quinientas empresas que se dedicaban a desarrollar, comercializar y vender esos productos a clientes gubernamentales[3].

Tipos de vigilancia que se tienen en cuenta en el presente informe

7. En el presente informe, el Relator Especial se ocupa principalmente de las tecnologías que permiten obtener acceso subrepticio a las comunicaciones digitales, los productos del trabajo, los datos de navegación, la investigación, el historial de localización y las actividades en línea y fuera de línea de las personas. A continuación se describen las principales tecnologías y prácticas de vigilancia selectiva.

Interferencia en el ordenador

8. Las tecnologías de vigilancia pueden permitir a los intrusos acceder al ordenador o a la red de un particular. El alcance de dicha interferencia es considerable[4]. Por ejemplo, en 2017, un tribunal de apelación de los Estados Unidos de América conoció de un caso de vigilancia organizada por un Estado extranjero en territorio de los Estados Unidos[5]. El caso se refería a un ciudadano estadounidense nacido en Etiopía y residente en el estado de Maryland que había venido prestando asistencia técnica a miembros de la comunidad de la diáspora etíope. Un documento enviado originalmente a un activista por agentes del Gobierno de Etiopía infectó su ordenador con un programa malicioso llamado FinSpy comercializado por una empresa germano-británica, Gamma Group[6]. FinSpy supuestamente grababa las videollamadas por Internet, los correos electrónicos y demás comunicaciones realizadas por ese hombre y su familia, incluso registrando las pulsaciones de su teclado, y enviaba los datos a servidores en Etiopía[7].

Piratería de dispositivos móviles

9. Los productos de que dispone la vigilancia privada también ofrecen la posibilidad de piratear directamente en dispositivos móviles. El programa espía Pegasus de NSO Group es un ejemplo paradigmático, y el análisis de su supuesta utilización en México resulta instructivo. A partir de 2015, numerosas personas que informaban sobre la corrupción y el

[2] Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society* (Toronto, Monk School of Global Affairs, Universidad de Toronto, 2014), Resumen Ejecutivo, págs. 8 a 11.

[3] Comunicación de Privacy International, pág. 1.

[4] Véase, por ejemplo, Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto, Signal, 2013), págs. 186 a 190.

[5] *Doe c. República Democrática Federal de Etiopía*, 851 F.3d 7 (D.C. Cir. 2017).

[6] El material promocional de FinSpy puede verse en Wikileaks, “The spy files: remote monitoring and infection solutions: FINSPY”.

[7] Pueden verse más detalles sobre las alegaciones en la *primera denuncia enmendada, Doe c. la República Democrática Federal de Etiopía* (18 de julio de 2014).

tráfico de drogas comenzaron a recibir mensajes de texto o enlaces en sus dispositivos móviles, algunos de los cuales provenían de fuentes aparentemente legítimas, lo que sugería un conocimiento detallado de los objetivos. Periodistas, políticos, investigadores de las Naciones Unidas, defensores de los derechos humanos y otras personas recibieron esos mensajes. Una organización canadiense de investigación y promoción, Citizen Lab, descubrió que esos enlaces habían infectado los dispositivos con el programa espía Pegasus, que permitía vigilar a los objetivos de forma remota. Citizen Lab ha determinado que el programa espía Pegasus se utiliza para vigilar selectivamente a personas en 45 países, entre ellos la Arabia Saudita, Bahrein, los Estados Unidos, el Reino Unido de Gran Bretaña e Irlanda del Norte y el Togo[8].

Ingeniería social

10. Muchas de las tecnologías descritas anteriormente van acompañadas de estrategias para conseguir que un objetivo descargue involuntariamente un programa malicioso en sus dispositivos. Por ejemplo, el remitente de los correos electrónicos que contienen enlaces maliciosos se hace pasar por un contacto del destinatario o lo engañan para que crea que está accediendo a un enlace benigno relacionado con su trabajo, ocio o asuntos personales. Por ejemplo, un mensaje de WhatsApp, que los investigadores vincularon al programa espía Pegasus, enviado a un miembro del personal de Amnistía Internacional instándole a que cubriera una protesta contenía un enlace que, supuestamente, permitía obtener información personal[9]. De haber accedido al enlace, es probable que el programa espía se hubiera instalado en su dispositivo.

Redes de vigilancia

11. Algunas tecnologías funcionan en red para permitir la vigilancia selectiva. Por ejemplo, el sistema de actividades operativas de investigación de Rusia entraña la instalación de un dispositivo en las redes de telecomunicaciones que permite interceptar las comunicaciones. El sistema se fabrica y comercializa en el sector privado y se utiliza ampliamente en la Federación de Rusia y otros lugares de Asia Central. La empresa Protei, por ejemplo, fabrica equipos que facilitan que las tecnologías del sistema, como los dispositivos de escucha e interceptación de Internet, funcionen en países como Uzbekistán y Kazajstán[10].

Reconocimiento facial y gestual

12. Mediante la tecnología de reconocimiento facial se pretende capturar y detectar las características faciales de una persona, lo que permitiría elaborar perfiles de personas sobre la base de su etnia, raza, origen nacional, género u otras características, que a menudo constituyen motivos ilícitos de discriminación[11]. Mediante el reconocimiento gestual se pretende detectar los sentimientos, emociones o intenciones de una persona a partir de sus expresiones faciales, basándose en sistemas de clasificación altamente cuestionables[12]. Tal vez ningún otro entorno demuestre mejor que China la intrusión general de esas tecnologías. Hay informes fidedignos que sugieren que el Gobierno de China, utilizando una combinación de tecnología de reconocimiento facial y cámaras de vigilancia en todo el país, "busca exclusivamente a los uigures sobre la base de su aspecto y mantiene registros de sus desplazamientos para su investigación y revisión"[13]. Gran parte de la tecnología

[8] Véase Bill Marczak y otros, "Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries", Citizen Lab, 18 de septiembre de 2018.

[9] Véase Bill Marczak, John Scott-Railton y Ron Deibert, "NSO Group infrastructure linked to targeting of Amnesty International and Saudi dissident", Citizen Lab, 31 de julio de 2018.

[10] Andrei Soldatov e Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (Nueva York, PublicAffairs, 2015), págs. 190 y 191.

[11] Véanse, por ejemplo, las comunicaciones de Internet Lab, pág. 6; y de Center for Internet and Society, pág. 12.

[12] AI Now Institute, *AI Now Report 2018* (Nueva York, Universidad de Nueva York, 2018), págs. 13 y 14.

[13] Véase Paul Mozur, "One month, 500,000 face scans: how China is using A.I. to profile a minority", *New York Times*, 14 de abril de 2019.

desplegada por el Gobierno parece ser de producción nacional, procedente tanto de empresas estatales como privadas[14].

Captadores de la Identidad Internacional de Suscriptor Móvil (Stingray)

13. Los captadores de la Identidad Internacional de Suscriptor Móvil imitan el comportamiento de las torres de telefonía móvil cercanas para interceptar las comunicaciones y los datos de localización que transmiten los dispositivos de comunicación personales. Esos captadores son ampliamente utilizados en todo el mundo, a menudo por las fuerzas del orden y los organismos de inteligencia. Una empresa privada del Reino Unido presuntamente vendió esos captadores y otros programas espía a Filipinas, y muchos temen que esos instrumentos se utilizaran para rastrear y vigilar a los consumidores de drogas en la ampliamente criticada guerra contra las drogas del Gobierno[15].

Inspección Profunda de Paquetes

14. La Inspección Profunda de Paquetes permite la vigilancia, el análisis y la redirección del tráfico que pasa por las redes de comunicaciones e Internet. También se puede utilizar para redirigir a los usuarios a sitios infectados con programas maliciosos y bloquear su acceso a determinados sitios web. Según se informa, esos dispositivos se instalaron en la red de Türk Telekom y se utilizaron para redirigir a los usuarios de Turquía y la República Árabe Siria para que descargasen programas espía cuando intentaban descargar aplicaciones legítimas[16].

Cooperación entre los sectores público y privado

15. Los gobiernos y el sector privado colaboran estrechamente en el mercado de los instrumentos para la vigilancia digital. Los gobiernos tienen necesidades que sus propios departamentos y agencias no pueden satisfacer. Las empresas privadas tienen los incentivos, la experiencia y los recursos necesarios para satisfacerlas. Se reúnen en ferias comerciales de ámbito mundial y regional diseñadas, como los servicios de citas, para que puedan juntarse[17]. A partir de ahí, determinan si pueden formar una pareja. Se desconoce si las empresas llevan a cabo algún tipo de diligencia debida para evaluar la trayectoria de los compradores en materia de derechos humanos.

16. Es posible que las intenciones del vendedor sean legítimas. Puede ser que las empresas pretendan de manera genuina que sus productos se utilicen para una "interceptación legal" por parte de las autoridades públicas autorizadas contra objetivos legítimos, con la autorización de las autoridades judiciales u otras autoridades independientes. Sin embargo, eso no se puede saber con certeza porque todos los aspectos de esa colaboración —desde la debida diligencia y las ventas hasta el apoyo al usuario final— suelen llevarse a cabo con una supervisión y una transparencia limitadas. De hecho, casi toda la información disponible públicamente sobre el sector de la vigilancia privada se ha recopilado gracias al trabajo forense llevado a cabo por instituciones no gubernamentales y académicas, como Citizen Lab, y durante la preparación de reportajes de investigación[18].

[14] Comunicación de Human Rights in China, págs. 2 y 3. Véase también A/HRC/39/29, párr. 14.

[15] Véase Sofia Tomacruz, "You think your data, communication devices are safe? Think again", Rappler, 17 de marzo de 2018.

[16] Véase Bill Marczak y otros, "Bad traffic: Sandvine's PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?", Citizen Lab, 9 de marzo de 2018.

[17] Véanse, por ejemplo, www.issworldtraining.com; y Patrick Howell O'Neill, "ISS World: the traveling spyware roadshow for dictatorships and democracies", Cyberscoop, 20 de junio de 2017.

[18] La historia de la vigilancia privada es también la historia de la importancia fundamental de la investigación y de los medios de comunicación libres e independientes. Esas investigaciones también han hecho que los investigadores corran el riesgo de ser ellos los vigilados. Véase, por ejemplo, Raphael Satter, "Undercover agents target cybersecurity watchdog", Associated Press, 26 de enero de 2019.

17. El funcionamiento del llamado “mercado de las vulnerabilidades” es especialmente turbio. Se sabe que los gobiernos y entidades privadas compran a quienes se dedican a investigar en el terreno de la seguridad vulnerabilidades presentes en programas informáticos de uso común para utilizarlas como “puertas de entrada de día cero” con el propósito de obtener acceso a comunicaciones y dispositivos personales[19]. Mientras el fabricante del dispositivo o del programa informático de que se trate no las conozca, las vulnerabilidades pueden servir como puertas de entrada para la vigilancia. Cuando los gobiernos y las empresas no revelan esas vulnerabilidades, ponen en peligro la seguridad de los usuarios, incluidos los clientes de los sectores público y privado que almacenan datos delicados sobre finanzas, salud, empleo o aplicación de la ley en bases de datos desarrolladas por las empresas. Hasta la fecha, no se ha llegado a un acuerdo sobre si los gobiernos y las empresas tienen la responsabilidad de compartir sus conocimientos sobre las vulnerabilidades, y la venta de esas vulnerabilidades sigue sin estar regulada. De hecho, la situación no solo ha facilitado el desarrollo de un valioso mercado de vulnerabilidades, sino que ha llevado a muchos gobiernos y empresas a guardar celosamente su conocimiento de las vulnerabilidades con la esperanza de poder utilizarlas con fines ofensivos[20].

18. También es evidente que la colaboración entre los sectores público y privado no termina en el punto de venta con la transferencia del producto. Documentos filtrados han demostrado que las empresas privadas de vigilancia proporcionan un servicio posventa. Por ejemplo, en 2014, FinFisher al parecer suscribió “contratos anuales de asistencia técnica” con clientes gubernamentales para proporcionar actualizaciones y mejoras técnicas de los productos y otras formas de asistencia al cliente[21]. También realizan actividades de formación sobre cómo optimizar el uso de sus programas maliciosos para comprometer las comunicaciones digitales, los dispositivos informáticos y las redes Wi-Fi de los objetivos de la vigilancia[22].

19. Del mismo modo que las empresas y los compradores están estrechamente vinculados, también lo están las empresas y los gobiernos de los países en los que están radicadas. Algunas de las empresas tienen una voz poderosa a la hora de diseñar los regímenes de control de las exportaciones de sus países y han socavado los esfuerzos para fortalecerlos. Por ejemplo, en 2016, se oyeron alegaciones creíbles que sugerían que, como resultado de la presión de los grupos de presión del sector, ciertas formas de tecnología de vigilancia se habían eliminado de una propuesta de adiciones a la lista de la Unión Europea de productos y tecnologías de doble uso sujetos a controles de exportación[23]. Durante las recientes negociaciones sobre el régimen de control de las exportaciones de la Unión Europea, se dijo que los intereses de las empresas parecían haber influido en la decisión de restringir significativamente la inclusión de salvaguardias de los derechos humanos en los cambios normativos propuestos, a pesar del amplio acuerdo sobre su adopción que se había logrado en el Parlamento Europeo[24].

20. También se ha indicado en informes recientes que muchas personas con conocimientos y experiencia en materia de inteligencia y aplicación de la ley se mueven entre puestos gubernamentales y del sector privado. Esa puerta giratoria puede permitir que antiguos expertos gubernamentales presten asistencia a entidades privadas cuyos productos

[19] Véase Privacy International, “Exploiting privacy: surveillance companies pushing zero-day exploits”, 7 de febrero de 2018.

[20] Véanse el debate en la comunicación de Sarah McKune, págs. 2 a 4; Centro de Estudios sobre Política Europea, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges* (Bruselas, junio de 2018); y Sven Herpig y Ari Schwartz, “The future of vulnerabilities equities processes around the world”, Lawfare, 4 de enero de 2019.

[21] Véase Privacy International, “Six things we know from the latest FinFisher documents”, 15 de agosto de 2014.

[22] *Ibid*.

[23] Véase Reporteros sin Fronteras, “International regulations: broken or blocked by lobbies”, 14 de marzo de 2017.

[24] Véase Daniel Moßbrucker, “Surveillance exports: how EU Member States are compromising new human rights standards”, netzpolitik.org, 29 de octubre de 2018.

pueden utilizarse para violar los derechos humanos[25]. En un informe de 2019, Reuters reveló que varios antiguos empleados de la Agencia de Seguridad Nacional de los Estados Unidos se pasaron a una empresa privada para prestar asistencia en la implantación de los programas de inteligencia de señales de los Emiratos Árabes Unidos bajo el nombre clave de "Project Raven"[26]. Los empleados en cuestión supuestamente aportaron sus conocimientos para vigilar a los opositores políticos de las autoridades de los Emiratos Árabes Unidos y observar a ciudadanos estadounidenses. La normativa gubernamental sobre la "puerta giratoria" con respecto al sector de la vigilancia privada parece, en el mejor de los casos, débil y probablemente inexistente en muchos, si no en la mayoría, de los sistemas legislativos.

III. Marco jurídico

A. Obligaciones de los Estados

21. Las personas señaladas para ser vigiladas sufren interferencias en sus derechos a la privacidad y a la libertad de opinión y de expresión, independientemente de que las actividades de vigilancia tengan éxito o no[27]. No es necesario que la persona vigilada tenga conocimiento de la intrusión, fallida o exitosa, para que la interferencia en su derecho a la privacidad sea completa. De hecho, por lo general, los gobiernos buscan instrumentos que permitan llevar a cabo la intrusión sin que la persona vigilada tenga conocimiento de ello. No obstante, es fundamental considerar esa interferencia como parte de un esfuerzo general para imponer al objetivo una situación determinada. Si se lleva a cabo con fines ilícitos, el intento de imponer la vigilancia —y la operación con éxito— puede utilizarse en un esfuerzo por silenciar la disidencia, sancionar las críticas o castigar la facilitación de información independiente (y castigar también a las fuentes de esa información)[28]. Las sanciones tal vez no se apliquen a los objetivos, sino a su red de contactos. En entornos sometidos a una vigilancia ilícita generalizada, las comunidades vigiladas conocen o sospechan de tales actividades, lo que a su vez perturba y restringe su capacidad para ejercer sus derechos a la libertad de expresión, asociación, creencia religiosa, cultura, etc. En resumen, la interferencia con la privacidad mediante la vigilancia selectiva está diseñada para reprimir el ejercicio del derecho a la libertad de expresión.

22. No es necesario duplicar la amplia actividad de presentación de informes sobre los derechos humanos que ya realizaron anteriores Relatores Especiales, otros titulares de mandatos, el ACNUDH, el Consejo de Derechos Humanos, el Comité de Derechos Humanos y otras entidades, informes en los que destacaron las características fundamentales del marco jurídico de derechos humanos que protege contra la vigilancia selectiva que se enumeran a continuación.

23. En primer lugar, tanto en el Pacto Internacional de Derechos Civiles y Políticos como en la Declaración Universal de Derechos Humanos se protege el derecho de toda persona a la intimidad y a la libertad de opinión y de expresión. En el artículo 19 de ambos instrumentos se protege el derecho de toda persona a tener sus propias opiniones y a buscar, recibir y difundir información e ideas de toda índole, sin limitación de fronteras y por cualquier procedimiento. En el párrafo 1 del artículo 17 del Pacto, que se hace eco del artículo 12 de la Declaración, se dispone que "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia".

[25] Véanse Privacy International, "Switching hats: why South Africa's surveillance industry needs scrutiny", 14 de diciembre de 2016; y Alex Kane, "How Israel became a hub for surveillance technology", The Intercept, 17 de octubre de 2016.

[26] Véanse Christopher Bing y Joel Schectman, "Inside the UAE's secret hacking team of American mercenaries", Reuters, 30 de enero de 2019; Robert Chesney, "Project Raven: what happens when U.S. personnel serve a foreign intelligence agency", Lawfare, 11 de febrero de 2019; y la comunicación de Sarah McKune, págs. 7 y 8.

[27] Comunicación de Global Justice Clinic, Facultad de Derecho de la Universidad de Nueva York, pág. 6.

[28] Véase la comunicación de la Human Rights Foundation.

24. La privacidad y la libertad de expresión están entrelazadas en la era digital, y la privacidad en línea es el punto clave para garantizar el ejercicio de la libertad de opinión y de expresión (A/HRC/29/32 y A/HRC/23/40, párr. 24). En virtud del artículo 17 las injerencias en el derecho a la intimidad se permiten solo cuando "estén autorizadas por una ley nacional que sea accesible y precisa y que se ajuste a los requisitos del Pacto", "tengan un objetivo legítimo" y "cumplan los criterios de necesidad y proporcionalidad" (A/69/397, párr. 30). En el artículo 19 se establece una prueba en tres partes en virtud de la cual se requiere que toda restricción debe estar fijada por la ley y ser necesaria y proporcionada para velar por los derechos o la reputación de los demás, la seguridad nacional, el orden público o la salud y la moral públicas[29]. El Comité de Derechos Humanos ha subrayado que esos principios significan, como mínimo, lo siguiente:

a) Fijada por la ley/legalidad: cualquier restricción debe estar formulada con precisión suficiente para que las personas puedan regular su comportamiento de conformidad con ella y hacerse accesible al público. La restricción no puede ser indebidamente vaga o demasiado amplia, de modo que pueda conferir a los funcionarios un poder discrecional ilimitado[30];

b) Necesidad y proporcionalidad: recae sobre el Estado la carga de probar que existe una conexión directa e inmediata entre la expresión y la amenaza y que la restricción que se pretende imponer es el instrumento menos intrusivo entre los que podrían lograr la misma función protectora[31];

c) Legitimidad: en el párrafo 3 del artículo 19 se imponen límites específicos a los intereses que justifican las restricciones. Si bien es habitual que los Estados traten de justificar las restricciones, especialmente la vigilancia selectiva, sobre la base de la seguridad nacional, el Relator Especial ha llegado a la conclusión de que esa lógica debe limitarse a las situaciones en que está en juego el interés de toda la nación, con lo que quedarían excluidas las restricciones que redunden exclusivamente en interés de un gobierno, un régimen o un grupo de poder (A/71/373, párr. 18).

25. El Comité de Derechos Humanos puso en práctica esos principios en sus observaciones finales de 2017 sobre el sexto informe periódico presentado por Italia en virtud del Pacto Internacional de Derechos Civiles y Políticos (CCPR/C/ITA/CO/6, párr. 36). En esas observaciones determinó que el derecho a la privacidad exigía que se pusieran en práctica unos sistemas sólidos e independientes de supervisión de la vigilancia, la interceptación y la piratería informática, y que se garantizase, en particular, que el poder judicial participase en la autorización de esas medidas en todos los casos y se ofreciesen a las personas afectadas recursos efectivos en caso de abuso, entre otros, cuando sea posible, una notificación *a posteriori* de que fueron objeto de medidas de vigilancia o de que sus datos quedaron comprometidos a causa de la piratería informática (*ibid*., párr. 37). La Asamblea General, en su resolución 73/179, se hizo eco de esos principios y señaló que la vigilancia de las comunicaciones digitales debía ser compatible con las obligaciones internacionales en materia de derechos humanos y basarse en un marco jurídico que debía ser accesible al público, claro, preciso, amplio y no discriminatorio.

26. Si bien esos principios se aplican en todos los casos de vigilancia selectiva, tienen una importancia especial cuando interviene la expresión en el interés público. La vigilancia selectiva incentiva la autocensura y menoscaba de manera directa la capacidad de los periodistas y los defensores de derechos humanos para realizar sus investigaciones y para forjar y mantener relaciones con sus fuentes de información (A/HRC/38/35/Add.2, párr. 53). El Comité ha hecho hincapié en que las restricciones nunca se pueden hacer valer como justificación para silenciar a los defensores de la democracia pluripartidista, los principios democráticos y los derechos humanos[32]. Los ataques a una persona a causa del ejercicio de su derecho a la libertad de expresión no pueden justificarse sobre la base de lo

[29] Una explicación detallada de la prueba en tres partes prevista en el artículo 19 puede verse en la observación general núm. 34 (2011) del Comité de Derechos Humanos, sobre la libertad de opinión y de expresión, párrs. 5 a 9 y 22 a 36; y en el documento A/HRC/38/35.

[30] Observación general núm. 34, párr. 25.

[31] *Ibid*., párrs. 34 y 35.

[32] Observación general núm. 34, párr. 23.

dispuesto en el párrafo 3 del artículo 19[33]. El Comité también señaló la importancia de proteger a los periodistas y a quienes reúnen y analizan información sobre la situación de los derechos humanos o publican informes sobre esos derechos, incluidos los jueces y los abogados[34]. Esa protección se extiende a la confidencialidad de las fuentes, que los mecanismos internacionales y regionales de derechos humanos (en los sistemas africano, europeo e interamericano) han destacado que deben protegerse en la legislación (A/70/361, párr. 5).

27. Además de la obligación primordial de no interferir en la vida privada ni restringir la libertad de expresión, los Estados también tienen la obligación de proteger a las personas contra la injerencia de terceros. En el artículo 2 del Pacto Internacional de Derechos Civiles y Políticos, en el que se recogen los deberes fundamentales de los Estados, se les impone la obligación de respetar y garantizar los derechos reconocidos en el Pacto a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción[35]. El párrafo 2 del artículo 17 del Pacto establece que toda persona tiene derecho a la protección de la ley frente a toda injerencia ilícita en su vida privada. Sin embargo, no está claro que los Estados ofrezcan en general una protección jurídica afirmativa contra la vigilancia selectiva. Eso es decididamente cierto en el caso de la vigilancia transnacional, incluso cuando los ciudadanos de un país son objeto de vigilancia por entidades extranjeras[36]. En un caso de denuncias de vigilancia selectiva en México, el Relator Especial sobre la libertad de expresión de la Comisión Interamericana de Derechos Humanos y el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión llevaron a cabo una misión conjunta al país en la que plantearon la cuestión de la utilización por el Gobierno del programa espía Pegasus. Instaron al Gobierno a que permitiera una investigación independiente de las denuncias de que se habían utilizado programas espía contra periodistas (A/HRC/38/35/Add.2, párrs. 52 a 55). Hasta la fecha, los esfuerzos por investigar esas denuncias no han aclarado la situación, a pesar de las órdenes del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México de que el Gobierno revelase la naturaleza de sus contratos para al adquirir el programa Pegasus[37],

28. De los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar", aprobados por el Consejo de Derechos Humanos en 2011, se desprende claramente que los Estados deben tomar medidas apropiadas para prevenir, investigar, castigar y reparar los abusos de los derechos humanos cometidos por terceros (A/HRC/17/31). En los Principios Rectores se insta a los Estados a que ejerzan una supervisión adecuada para cumplir sus obligaciones internacionales en materia de derechos humanos cuando contraten a empresas comerciales, o legislen en su favor, para prestar servicios que puedan tener repercusiones en el disfrute de los derechos humanos (*ibíd*., pág. 10).

B. Responsabilidad de las empresas

29. Debido a que las empresas del sector de la vigilancia privada operan bajo un manto de secretismo, el público carece de información sobre la forma en que esas empresas determinan —suponiendo que lo hagan— el impacto de sus productos en los derechos

[33] *Ibid*.

[34] *Ibid*.

[35] Véase también Comité de Derechos Humanos, observación general núm. 31 (2004), sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto. Obsérvese que, en la observación general núm. 31, el artículo 17 sobre la privacidad se incluye específicamente como ejemplo de un artículo en relación con el cual los Estados partes tienen la obligación positiva de intervenir en las actividades de las personas o entidades privadas.

[36] Véase Nate Cardozo, "D.C. circuit court issues dangerous decision for cybersecurity: Ethiopia is free to spy on Americans in their own homes", Electronic Frontier Foundation, 14 de marzo de 2017.

[37] Véanse Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Fiscalía general de la República tiene oportunidad histórica para acabar con la impunidad en caso Pegasus: Salas Suárez", 27 de marzo de 2019; y Juan Arvizu, "Ordena Inai a PGR abrir contrato de compra de Pegasus", *El Universal*, 17 de abril de 2018.

humanos. Dada la naturaleza del sector y el uso generalizado de sus productos para fines incompatibles con el derecho internacional de los derechos humanos, es difícil imaginar que en realidad tengan en cuenta ese impacto. Dicho de otro modo: dado el amplio conocimiento público de la represión que practican muchos de sus clientes, las empresas no pueden pretender que les tomen en serio cuando afirman que no tienen conocimiento del uso represivo de sus productos.

30. Los Principios Rectores proporcionan un marco para evaluar si las empresas de vigilancia respetan los derechos de las personas afectadas por sus productos y servicios. En particular, en los Principios Rectores se hace hincapié en los compromisos de política de respetar los derechos humanos; los procesos de diligencia debida que permitan identificar, prevenir, mitigar el impacto en los derechos humanos; la consulta con los grupos afectados; la evaluación continua de la eficacia de las políticas de derechos humanos; y el establecimiento de mecanismos eficaces de reclamación para los titulares de derechos afectados (A/HRC/17/31, párrs. 15 a 25).

31. En cualquier caso, las empresas parecen no cumplir ni siquiera esos mínimos de referencia. Las pocas empresas que han publicado sus políticas para con los clientes hacen una referencia vaga ante la necesidad de respetar los derechos humanos. Hacking Team, por ejemplo, dice que "analiza a los posibles clientes antes de una venta para determinar si hay o no pruebas objetivas o preocupaciones genuinas de que la tecnología que Hacking Team pretende proporcionar se utilizará para facilitar la violación de los derechos humanos", pero no explica qué hace con dicha información, ni siquiera menciona a qué derechos humanos podrían afectar sus tecnologías[38]. NSO Group afirma que opera guiado por un Comité de Ética Empresarial, "que incluye expertos externos de varias disciplinas, como el derecho y las relaciones exteriores", y sugiere que puede cancelar un trabajo si detecta que a sus productos se les va a dar un "uso indebido"[39]. En su sitio web también afirma que "investigará cualquier denuncia creíble de uso indebido de sus productos", pero no hay ninguna indicación de si eso incluye la vulneración de los derechos humanos[40].

32. En resumen, las empresas no han comunicado casos en que hayan adoptado medidas significativas, como la puesta en marcha de procesos de diligencia debida que sirvan para identificar y evitar causar o contribuir a unos efectos adversos de sus propias actividades en los derechos humanos y para prevenirlos o mitigarlos cuando estén directamente vinculados a sus operaciones, productos o servicios en virtud de sus relaciones comerciales (A/HRC/17/31, anexo, principio 13). Por ejemplo, no hay ninguna información pública que sugiera que las evaluaciones desde la óptica de los derechos humanos sean un componente habitual de los procesos de diligencia debida durante las ventas, que las empresas den un peso decisivo a esas evaluaciones o que esas evaluaciones se mantengan a lo largo del ciclo de vida del producto y del contrato de servicios posventa. De hecho, la creciente evidencia del papel fundamental del sector en la facilitación de graves vulneraciones de los derechos humanos, junto con su firme negativa a explicar sus salvaguardias, hace difícil evitar la conclusión de que dicha autorregulación carece de cualquier valor.

33. En las directrices de la Comisión Europea sobre la aplicación de los Principios Rectores en el sector de la tecnología de la información y las comunicaciones pone de relieve la importancia que reviste tener en cuenta los "derechos humanos desde el diseño"[41]. El riesgo extraordinario de mal uso de los productos de vigilancia significa que las empresas deben anticipar el uso ilícito de sus programas y comenzar a diseñar soluciones para reparar los inevitables impactos negativos. En un gesto prometedor, el Gobierno del Reino Unido, en colaboración con una asociación del sector tecnológico, ha elaborado un

[38] Hacking Team, Política para con el cliente.

[39] Véase la declaración de NSO de 17 de septiembre de 2018. Puede consultarse en https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf. Como dice Citizen Lab, "las declaraciones de NSO sobre un Comité de Ética Empresarial recuerdan el ejemplo del 'panel externo de expertos técnicos y asesores legales' de Hacking Team... que analizan las posibles ventas. Ese 'panel externo' parece haber sido un único bufete de abogados, cuyas recomendaciones Hacking Team no siempre siguió" (Marczak y otros, "Hide and seek").

[40] Véase www.nsogroup.com/about.

[41] Véase Comisión Europea, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (Luxemburgo, 2013).

conjunto de directrices para el sector de la ciberseguridad en el que se destaca la importancia de prevenir y mitigar los riesgos para los derechos humanos "mediante una modificación apropiada del diseño" en las primeras etapas del desarrollo de un producto.

C. Control de las exportaciones a nivel nacional e internacional

34. Los controles de la exportación son un elemento importante del esfuerzo por reducir los riesgos causados por el sector de la vigilancia privada y el uso de sus productos para la represión. Sin embargo, su efectividad es limitada. En primer lugar, el régimen internacional de control de las exportaciones pertinente —el Arreglo de Wassenaar sobre el Control de las Exportaciones de Armas Convencionales y Bienes y Tecnologías de Doble Uso, en el que participan 42 Estados— está concebido para reducir las amenazas a la seguridad regional e internacional. Si bien se trata de un objetivo loable y necesario, no es el marco adecuado para hacer frente a las amenazas que la vigilancia selectiva plantea para los derechos humanos; de hecho, carece de directrices o medidas de vigilancia del cumplimiento que aborden directamente las violaciones de los derechos humanos causadas por los instrumentos de vigilancia. En segundo lugar, el interés exclusivo en las exportaciones es una forma imperfecta de abordar el problema principal: el uso de esas tecnologías para socavar la expresión lícita, la disidencia, la denuncia pública y otros ejemplos del ejercicio de los derechos humanos.

35. No obstante, el Arreglo de Wassenaar promueve importantes objetivos de "transparencia y mayor responsabilidad en las transferencias de armas convencionales y de bienes y tecnologías de doble uso". Se espera que los Estados participantes apliquen controles a la exportación de todos los productos incluidos en la lista de bienes y tecnologías de doble uso, por lo que el Arreglo ha sido (o debería ser) incorporado en la legislación y las políticas nacionales de los Estados participantes y de algunos Estados no participantes[42]. Lamentablemente, no existe un mecanismo de vigilancia del cumplimiento que garantice su incorporación a la legislación nacional o su aplicación por parte de los organismos nacionales pertinentes.

36. En 2013, los Estados participantes añadieron a la lista de tecnologías de doble uso los productos relacionados con los "programas informáticos intrusivos" y los sistemas de vigilancia de las comunicaciones de redes con el Protocolo de Internet. Según la lista, se consideran programas informáticos intrusivos "los 'programas' especialmente diseñados o modificados para evitar ser detectados por 'herramientas de supervisión', o para evitar las 'contramedidas de protección'", que extraen datos de un ordenador o de un dispositivo de red o modifican el "proceso de ejecución estándar" de un programa para permitir "la ejecución de instrucciones provenientes del exterior"[43].

37. Hay informes detallados de abusos relacionados con la vigilancia que demuestran que el régimen de control de las exportaciones centrado en el Arreglo de Wassenaar no ha limitado de manera sensible la difusión de las tecnologías de vigilancia y su utilización con fines represivos. El estancamiento de los esfuerzos de los parlamentarios europeos por fortalecer la protección de los derechos humanos en las leyes y políticas europeas relativas a las exportaciones demuestra las dificultades que supone la reforma. Su voluntad era la de exigir explícitamente la ampliación de la lista de productos de doble uso y controles generales, así como la consideración del "respeto de los derechos humanos en el país de destino final" de las tecnologías de vigilancia[44]. En enero de 2018, esa propuesta se sometió a primera lectura en el Parlamento Europeo, y en un principio obtuvo apoyo suficiente para imponer la aplicación de controles más estrictos a las exportaciones de tecnología de doble

[42] Véase el Arreglo de Wassenaar, "Lista de municiones y productos y tecnologías de doble uso".

[43] *Ibid*., pág. 221.

[44] Véanse Comisión Europea, "Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establece un régimen de la Unión de control de las exportaciones, la transferencia, el corretaje, la asistencia técnica y el tránsito de productos de doble uso (versión refundida)", 28 de septiembre de 2016; y Lucie Krahulcova, "The European Parliament is fighting to strengthen the rules for surveillance trade", Access Now, 8 de diciembre de 2017.

uso[45]. Sin embargo, desde entonces la propuesta ha recibido críticas de al menos nueve Estados miembros, que abogan por imponer un menor nivel de protección de los derechos humanos[46]. El futuro de la legislación es ahora incierto[47].

38. A nivel nacional, la aplicación de los controles de exportación varía, incluso entre los Estados participantes en el Arreglo de Wassenaar. Por ejemplo, los Estados Unidos aún no han adoptado las adiciones de elementos relacionados con los programas informáticos intrusivos y los sistemas de vigilancia de las comunicaciones de red con Protocolo de Internet incorporadas en 2013[48]. Sin embargo, el Departamento de Comercio de los Estados Unidos está llevando a cabo una amplia revisión del marco actual y ha recibido el encargo de establecer un proceso interinstitucional para establecer nuevos controles tanto para las tecnologías "emergentes" como para las "fundacionales" en virtud de la Ley de Reforma del Control de las Exportaciones de 2018[49]. Israel, un Estado no participante, ha adoptado controles de la exportación de productos de doble uso regulados por el Arreglo de Wassenaar, pero su aplicación de esos controles está envuelta en un velo de secretismo[50].

D. Ausencia de soluciones para la vigilancia selectiva

39. Como parte del deber del Estado de respetar y garantizar el disfrute de los derechos humanos, en el apartado a) del párrafo 3 del artículo 2 del Pacto Internacional de Derechos Civiles y Políticos se impone la obligación de proporcionar a las víctimas de violaciones de los derechos acceso a un recurso efectivo. En el apartado b) del párrafo 3 del artículo 2 se especifica que las denuncias de esas violaciones deben ser sustanciadas por las autoridades judiciales, administrativas o legislativas competentes, o por cualquier otra autoridad competente prevista en el ordenamiento jurídico del Estado. El Comité de Derechos Humanos ha subrayado que las fuerzas del orden y la fiscalía deben investigar las denuncias de violaciones de manera rápida, exhaustiva y eficaz por conducto de órganos independientes e imparciales[51]. El deber de proporcionar recursos efectivos también entraña la obligación de proteger a las personas frente a los actos de entidades del sector privado que causen infracciones, ejerciendo la diligencia debida para prevenir, castigar, investigar o reparar el daño causado por tales actos realizados por personas o entidades privadas[52].

40. Las víctimas de la vigilancia selectiva han tenido poco éxito en sus esfuerzos por obtener el reconocimiento del daño sufrido, por no hablar de la reparación de ese daño. Ello es así a pesar de que, como han explicado tanto el Tribunal Europeo de Derechos Humanos como el ACNUDH, la mera amenaza de someter a alguien a vigilancia, incluso cuando es secreta, junto con la falta de reparación, puede constituir una injerencia en el derecho a la intimidad[53].

41. El recurso a los tribunales como medio para buscar soluciones contra las empresas privadas de vigilancia que fabrican y venden los productos y contra los gobiernos que los utilizan es incierto. La falta de motivos legales para presentar querellas y la ausencia de

[45] En EUR-Lex, Doc.52016PC0616 puede consultarse una visión general de la trayectoria legislativa de la propuesta de reglamento antes mencionada,

[46] Delegaciones de Chipre, Estonia, Finlandia, Irlanda, Italia, Polonia, Suecia, el Reino Unido y la República Checa, "For adoption of an improved EU Export Control Regulation 428/2009 and for cyber-surveillance controls promoting human rights and international humanitarian law globally", WK 5755/2018 INIT (15 de mayo de 2018); y Access Now, "EU: States push to relax rules on exporting surveillance technology to human rights abusers", 11 de junio de 2018.

[47] Véanse Catherine Stupp, "Nine countries united against EU export controls on surveillance software", Euractiv, 11 de junio de 2018; y Moßbrucker, "Surveillance exports".

[48] Comunicación de Privacy International, pág. 5.

[49] John S. McCain, National Defense Authorization Act for Fiscal Year 2019, Public Law núm. 115-232 (2018).

[50] Véase "Israel-U.S. export controls", export.gov, 20 de julio de 2018. Véase también el párr. 43 del presente documento.

[51] Observación general núm. 31, párr. 15.

[52] *Ibid*., párr. 8.

[53] Tribunal Europeo de Derechos Humanos, *Roman Zakharov c. Rusia*, (demanda núm. 47143/06), fallo de 4 de diciembre de 2015, párr. 171, y A/HRC/27/37, párr. 20.

recursos plantea graves preocupaciones acerca de la posibilidad de que las empresas rindan cuentas por las violaciones de los derechos humanos. Algunas presuntas víctimas han recurrido a los tribunales o han presentado denuncias oficiales contra empresas privadas de vigilancia o gobiernos en al menos ocho países[54]. Sin embargo, los obstáculos que dificultan el éxito de las reclamaciones judiciales y las denuncias formales son importantes, y entre ellos cabe citar la falta de supervisión judicial, de recursos, de motivos legales para presentar querellas, de medidas para la observancia de la ley y de conservación de datos.

42. En algunos casos, las organizaciones de la sociedad civil han pedido a los gobiernos que investiguen las actividades de vigilancia ilícita, pero con frecuencia se rechazan esas solicitudes. En el Reino Unido, Privacy International presentó una querella contra Gamma Group ante el Organismo Nacional contra la Delincuencia, alegando que la empresa había violado múltiples leyes nacionales cuando su filial, FinFisher, vendió tecnologías de vigilancia y prestó asistencia al Gobierno de Bahrein[55]. El European Centre for Constitutional and Human Rights y Privacy International también presentaron una querella en Munich (Alemania) en la que pedían que se investigara a la empresa, pero la fiscalía rechazó la solicitud[56]. Incluso cuando los Estados abren investigaciones para determinar si las actividades de vigilancia de los Gobiernos han vulnerado las normas de derechos humanos o las leyes estatales, las investigaciones pueden ser arbitrarias o desorganizadas.

43. No parece haber alternativas a recurrir a los tribunales que ofrezcan reparaciones compatibles con el derecho internacional de los derechos humanos. Por ejemplo, a raíz de que un miembro del personal de Amnistía Internacional recibiera un mensaje sospechoso de WhatsApp supuestamente relacionado con Pegasus, la organización escribió al Ministerio de Defensa de Israel solicitando la revocación de la licencia de exportación de NSO Group[57]. El Organismo de Control de las Exportaciones de Defensa del país respondió con una carta en la que afirmaba que no proporcionaba información sobre sus políticas de concesión de licencias de exportación ni sobre las licencias propiamente dichas[58]. El Organismo no confirmó ni negó la existencia de la licencia de exportación, pero sí señaló que "las licencias de exportación expedidas por el [Ministerio de Defensa] israelí a NSO Group en relación con sus clientes gubernamentales son compatibles con las obligaciones internacionales"[59]. La falta de presión a nivel regional e internacional y las políticas de no divulgación justificadas sobre la base de la seguridad nacional resultan ser obstáculos importantes.

44. Privacy International también ha presentado denuncias contra Gamma y Trovicor ante los centros nacionales de coordinación de Alemania y el Reino Unido en la Organización de Cooperación y Desarrollo Económicos (OCDE) por su presunta participación en la vigilancia selectiva de opositores políticos por parte del Gobierno de Bahrein[60]. En la denuncia contra Trovicor se pedía al centro nacional de coordinación de Alemania que "averiguara si la empresa había violado las Líneas Directrices de la OCDE para Empresas Multinacionales al exportar productos de vigilancia a Bahrein, donde las autoridades utilizan dichos productos para cometer abusos de los derechos humanos, incluidos la detención, el encarcelamiento y la tortura de disidentes y opositores

[54] Véase Siena Anstis, "Litigation and other formal complaints concerning targeted digital surveillance and the digital surveillance industry", Citizen Lab, 12 de diciembre de 2018.

[55] Véase Privacy International, "Criminal complaint to national cyber crime unit on behalf of Bahraini activists", 13 de octubre de 2014. También se han presentado demandas contra NSO Group en Israel y Chipre: véase David D. Kirkpatrick y Azam Ahmed, "Hacking a prince, an emir and a journalist to impress a client", *New York Times*, 31 de agosto de 2018.

[56] Véase European Centre for Constitutional and Human Rights, "FinFisher: no investigation into German-British software company", 12 de diciembre de 2014.

[57] Comunicación de Amnistía Internacional, pág. 8.

[58] *Ibid*.

[59] *Ibid*.

[60] Según el sitio web de la organización, el papel principal de un centro nacional de coordinación "es promover la eficacia de las Líneas Directrices mediante actividades de promoción, la tramitación de solicitudes y la contribución a la resolución de los problemas que puedan surgir de la supuesta inobservancia de las directrices en casos concretos".

políticos”[61]. Sin embargo, el centro nacional de coordinación rechazó la denuncia por considerar que las pruebas de la presencia de Trovicor en Bahrein no eran suficientes. En una denuncia prácticamente idéntica presentada ante el centro nacional de coordinación del Reino Unido, varias organizaciones de la sociedad civil alegaron violaciones similares contra Gamma[62]. El centro nacional de coordinación aceptó tramitar la denuncia y publicó una evaluación inicial en junio de 2013, en la que se afirmaba que: “aunque ninguna de las partes ha proporcionado pruebas directas sobre las ventas de Gamma a Bahrein, las pruebas aportadas sugieren que el producto vendido por la empresa puede haber sido utilizado contra activistas bahreiníes. El [centro nacional de coordinación] considera que eso corrobora las cuestiones relativas a las obligaciones de la empresa de actuar con la debida diligencia y de tener en cuenta los impactos”[63].

45. Aunque en el informe final del centro nacional de coordinación se formularon varias recomendaciones basadas en las normas de derechos humanos, no hay pruebas de que Gamma las haya aplicado, ni siquiera incluso de que haya reconocido el informe[64].

IV. Marco para la protección de los derechos fundamentales contra la vigilancia selectiva

46. Decir 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. Si bien en las normas de derechos humanos se imponen restricciones específicas al uso de los instrumentos de vigilancia, los Estados practican la vigilancia ilícita sin temor alguno a las consecuencias legales. Hay un marco jurídico de derechos humanos en vigor, pero no hay un marco similar para hacer cumplir las limitaciones al uso de los instrumentos de vigilancia. Es imperativo, urgentemente imperativo, que los Estados limiten los usos de esas tecnologías a aquellos que sean lícitos, con sujeción a las formas más estrictas de supervisión y autorización, y que condicionen la participación del sector privado en el mercado de los instrumentos de vigilancia —desde la investigación y el desarrollo hasta la comercialización, la venta, la transferencia y los servicios de asistencia— a la actuación con la diligencia debida en materia de derechos humanos y a la adquisición de un historial de observancia de las normas de derechos humanos.

47. El anterior titular del mandato insistió en que los Estados debían adoptar medidas para impedir la comercialización de las tecnologías de vigilancia, prestando especial atención a la investigación, el desarrollo, el comercio, la exportación y el uso de esas tecnologías, teniendo en cuenta su capacidad para facilitar la violación sistemática de los derechos humanos (A/HRC/23/40, párr. 97). Ese llamamiento sigue manteniendo su vigencia hoy en día. En la presente sección, el Relator Especial examina los principales elementos de un marco para proteger a las personas frente a los usos de la tecnología de vigilancia que interfieren con el disfrute de los derechos humanos. Las medidas propuestas en el presente informe requieren la adopción y aplicación de medidas por los Estados, en su calidad de usuarios de esas tecnologías y de países exportadores; por las empresas, de conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos; de manera conjunta por los Estados y las empresas en colaboración con la sociedad civil; y por el Consejo de Derechos Humanos,

[61] Véase Privacy International, “OECD complaint: Trovicor exporting surveillance technology to Bahrain”, 1 de febrero de 2013.

[62] Véase Privacy International, “German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain”, 20 de diciembre de 2013.

[63] Reino Unido, Departmento de Innovación y Aptitudes Empresariales, “Initial assessment by the UK National Contact Point for the OECD Guidelines for Multinational Enterprises: complaint from Privacy International and others against Gamma International UK Limited, June 2013” (Londres, 2013), párr. 25.

[64] Véanse Amitpal Singh, “OECD finds actions of Gamma International to be in violation of human rights”, Citizen Lab, 3 de marzo de 2015; y “UK National Contact Point for the OECD Guidelines for Multinational Enterprises – Privacy International y Gamma International UK Ltd: final statement after examination of complaint”, diciembre de 2014.

A. Moratoria de la exportación y el uso de tecnologías para la vigilancia selectiva

48. Las empresas privadas están creando, transfiriendo y prestando servicios de asistencia —y los Estados están comprando y utilizando— tecnologías de vigilancia de una forma que genera motivos de preocupación. Se han presentado denuncias creíbles que han demostrado que las empresas están vendiendo sus productos a gobiernos que los utilizan para poner en el punto de mira a periodistas, activistas, personalidades de la oposición y otras personas que desempeñan un papel fundamental en la sociedad democrática. Algunas de esas empresas refutan esas denuncias, alegando que no permiten el uso de sus productos con fines ilícitos, que disponen de mecanismos para evaluar las ventas a usuarios finales "sensibles" y que respetan las leyes nacionales sobre el control de las exportaciones. Es posible que las empresas intenten de manera genuina hacer frente a las acusaciones de complicidad en la represión y los abusos basados en la vigilancia. Sin embargo, no hay ninguna razón para aceptar la palabra de las empresas privadas sin que se sometan previamente a procesos de divulgación pública y rendición de cuentas. La gravedad de las acusaciones exige transparencia en las relaciones y los procesos de las empresas, por no mencionar una serie de otras medidas que se describen a continuación.

49. La aplicación de las medidas que figuran en el presente informe llevará tiempo. Entretanto, decenas de periodistas, activistas, defensores de los derechos humanos y críticos del sistema estarán a merced de unos gobiernos envalentonados por toda la gama de instrumentos de vigilancia altamente intrusivos que tienen a su disposición. Así pues, es esencial que las empresas dejen inmediatamente de vender, transferir y prestar servicios de asistencia para esas tecnologías hasta que hayan proporcionado pruebas convincentes de que han adoptado medidas suficientes (como se indica más adelante) en relación con la diligencia debida, la transparencia y la rendición de cuentas para impedir que esas tecnologías se utilicen para cometer abusos de los derechos humanos o para mitigar sus efectos. Los gobiernos también deben imponer una moratoria inmediata a la concesión de licencias para la exportación de tecnologías de vigilancia hasta que haya pruebas convincentes de que se dispone de medios técnicos para restringir el uso de esas tecnologías a fines lícitos que sean compatibles con las normas de derechos humanos, o de que esas tecnologías solo se exportarán a países en los que su uso esté sujeto a la autorización —otorgada de conformidad con las debidas garantías procesales y las normas de legalidad, necesidad y legitimidad— de un órgano judicial independiente e imparcial. Por ahora, sin embargo, la creciente evidencia de que los instrumentos de vigilancia desarrollados por el sector privado se están utilizando con fines manifiestamente ilegítimos constituye un sólido argumento a favor de una moratoria de estas transferencias.

B. Obligaciones de los gobiernos como usuarios de las tecnologías de vigilancia

1. Reforzar las leyes nacionales que limitan la vigilancia de conformidad con las obligaciones dimanantes del derecho internacional de los derechos humanos

50. Como primera medida, los gobiernos que utilicen instrumentos de vigilancia deben asegurarse de que lo hacen dentro de un marco jurídico nacional que satisfaga los requisitos exigidos en virtud de las normas internacionales de derechos humanos. La vigilancia debe estar autorizada por ley, que solo lo hará en el caso de los delitos más graves. Para cumplir con esos requisitos, en las leyes nacionales se debe:

a) Hacer hincapié en que toda persona tiene derecho a no ser objeto de intrusiones ilegales o arbitrarias en su vida privada, a mantener sus propias opiniones sin injerencias y a buscar, recibir y difundir información e ideas sin limitación de fronteras y por cualquier medio;

b) Exigir que cualquier normativa que regule las actividades de vigilancia esté contenida en leyes precisas y públicamente accesibles y solo se aplique cuando sea necesario y de manera proporcionada para lograr alguno de los objetivos legítimos

enumerados en el párrafo 3 del artículo 19 del Pacto Internacional de Derechos Civiles y Políticos;

c) Velar por que una operación de vigilancia sobre una persona concreta solo se pueda aprobar cuando sea compatible con el derecho internacional de los derechos humanos y haya sido autorizada por un órgano judicial competente, independiente e imparcial, con todas las limitaciones procedentes en cuanto a su duración, forma, lugar y alcance;

d) Exigir, dados los riesgos extremos de abuso asociados con las tecnologías de vigilancia selectiva, que los usos autorizados estén sujetos a estrictos requisitos de mantenimiento de registros. Las solicitudes de vigilancia solo deben aprobarse en el marco de unos procedimientos jurídicos regulares y documentados y han de culminar con la expedición de órdenes judiciales para tal fin. Deberá notificarse a la persona la decisión de autorizar su vigilancia tan pronto como dicha notificación no ponga en peligro el propósito de la medida[65].

51. Es habitual que los Estados impongan una pesada carga de prueba a las investigaciones penales que tratan de acceder a la labor de los periodistas (A/70/361, párr. 24). Las tecnologías de vigilancia se utilizan a menudo contra aquellos que desempeñan un papel importante en la promoción de los valores democráticos. El Relator Especial reconoce que algunos Estados pueden creer que hay situaciones en que, por ejemplo, los periodistas utilizan la cobertura de su profesión para cometer graves delitos. En su experiencia, esas afirmaciones son casi siempre falsas o exageradas. Con demasiada frecuencia, los gobiernos utilizan ese tipo de afirmaciones para socavar el periodismo y amordazar las voces disidentes o para vigilar a los periodistas, incluso cuando no son objeto de una investigación penal legítima, lo que afecta de manera desproporcionada a la libertad de prensa. En ese contexto, la posición por defecto de la ley debe ser la de prohibir el uso de instrumentos de vigilancia digital contra las personas que trabajan en los medios de comunicación. Por supuesto, eso no significa que los periodistas deban tener inmunidad frente a otros procedimientos legales legítimos, incluida la vigilancia no digital. Se trata simplemente de que, en el contexto de las tecnologías intrusivas de vigilancia digital, la posibilidad de abuso o "filtración" de una investigación penal legítima hacia ámbitos relacionados con otras labores periodísticas es muy real y difícil de contener, cuando no imposible. Es probable que esa posibilidad real sirva para disuadir a los periodistas de trabajar en los temas más delicados, por no hablar de la voluntad de las fuentes y de los denunciantes de irregularidades de dar un paso al frente.

2. Establecer mecanismos públicos para la aprobación y supervisión de las tecnologías de vigilancia

52. La autorización judicial para que un gobierno pueda utilizar las tecnologías de vigilancia es necesaria pero no suficiente. La adquisición de esas tecnologías también debe estar sujeta a una supervisión, una consulta y un control públicos genuinos. En los últimos años, a medida que el uso de las tecnologías de vigilancia ha proliferado entre las fuerzas del orden en los Estados Unidos, varias comunidades han instituido juntas de control civil para regular su adquisición y uso. La ciudad de Oakland (California), por ejemplo, aprobó una ordenanza que contenía varias características relacionadas con la adquisición de tecnología de vigilancia que podría ser tomada como modelo por otros estados[66]. Entre esas características cabe mencionar las siguientes:

a) Un proceso de aprobación, gestionado por los departamentos pertinentes, que tiene en cuenta las obligaciones del Estado en materia de derechos humanos;

b) La notificación pública de esas adquisiciones mediante los procesos ordinarios y la celebración de consultas públicas sobre cuestiones como los posibles

[65] Véase "Necessary and proportionate: International Principles on the Application of Human Rights to Communications Surveillance" (mayo de 2014).

[66] Véase American Civil Liberties Union of Northern California, "Oakland becomes latest municipality to reclaim local control over surveillance technologies used by local law enforcement", 2 de mayo de 2018.

impactos de esas adquisiciones en los derechos humanos y la eficacia de las tecnologías en cuestión para lograr los fines previstos;

c) La elaboración de informes públicos periódicos sobre dichas aprobaciones, compras y usos.

53. En particular, en los Estados en que se permite a los órganos subnacionales cierta autonomía en la compra de instrumentos para hacer cumplir la ley, debe alentarse y vigilarse el control comunitario de esas compras. Dado el claro interés del público en mantener la privacidad y la seguridad de los programas informáticos comerciales ampliamente disponibles, los mecanismos de supervisión pública también deben estar facultados para establecer políticas sobre el almacenamiento de vulnerabilidades y el desarrollo de las correspondientes puertas de entrada.

3. Proporcionar a las víctimas instrumentos jurídicos de reparación a nivel nacional

54. Por las razones descritas anteriormente, es difícil que las personas que se convierten en objetivos de la vigilancia ilícita o arbitraria presenten denuncias contra los gobiernos. Algunas de las barreras son estructurales, como la imposibilidad en muchos sistemas legales de presentar denuncias contra entidades gubernamentales. Tanto las legislaturas como los tribunales también pueden prohibir esas demandas cuando protegen excesivamente los supuestos intereses de la seguridad nacional y de la aplicación de la ley. Algunas reclamaciones pueden ser difíciles de tramitar debido a la dificultad y el costo que supone probar la existencia de la vigilancia o atribuirla a agentes del Estado, o incluso a organismos estatales específicos que pudieran ser objeto de una demanda. Los individuos vigilados a menudo no saben que se les está vigilando o, en otro caso, puede que hayan llegado a saberlo cuando los posibles delitos ya habían prescrito[67]. En otras palabras, es extremadamente raro que un demandante tenga éxito en una demanda judicial nacional derivada de una vigilancia presuntamente ilícita.

55. Los Estados que se toman en serio el uso indebido de las tecnologías de vigilancia deben adoptar medidas que permitan a los particulares presentar denuncias contra entidades estatales y no estatales. Para muchos Estados, eso entrañará necesariamente garantizar que las normas relativas a la jurisdicción, las pruebas, la prescripción y otros requisitos básicos sean adecuadas para los fines que se persigue en la era digital. Por ejemplo, deben velar por que los tribunales puedan aceptar y evaluar como prueba el análisis forense de los expertos técnicos. En la legislación nacional también se deben establecer motivos de denuncia contra las entidades privadas en los que se tengan en cuenta los cambios en la propiedad de las empresas (conocidos como “cesiones” o “transformaciones”), que a menudo complican los esfuerzos de las víctimas por asignar la responsabilidad y obtener reparación[68]. También deben considerarse formas alternativas de reparación, como las comisiones de la verdad que facilitan el testimonio de las víctimas de violaciones graves de los derechos humanos facilitadas por la vigilancia digital y que permiten analizar la complicidad de las empresas en esos abusos.

56. Al mismo tiempo, la vigilancia selectiva no siempre está limitada territorialmente. Cuando los Estados van más allá de sus fronteras para llevar a cabo una vigilancia selectiva, puede resultar difícil para las personas vigiladas presentar denuncias contra el Estado infractor. En esos casos, también pueden existir las mismas cargas probatorias y de otro tipo que en las reclamaciones nacionales. Además, como sucedió en el caso *Doe* mencionado anteriormente, los tribunales pueden no estar dispuestos a considerar demandas contra sujetos de soberanía extranjera. Si bien las normas aplicables a esas demandas varían, los Estados deben interpretar las normas de inmunidad soberana de manera que sus tribunales puedan admitir demandas contra gobiernos extranjeros.

[67] Véase *Roman Zakharov c. Rusia*.

[68] Comunicación de Access Now, pág. 8.

C. Obligaciones de los gobiernos que conceden licencias de exportación de tecnología de vigilancia

57. El Arreglo de Wassenaar no constituye la última palabra en lo que se refiere al control de las exportaciones de tecnologías de vigilancia. La utilidad de las listas de control depende de su aplicación a nivel nacional. El Arreglo tampoco cuenta con la participación de los principales países exportadores: Israel, uno de los principales actores en el mercado de la tecnología de vigilancia, afirma que "cumple plenamente" con el Arreglo, aunque todavía no participa en él[69]. También es cierto que el Arreglo ofrece un marco limitado, ya que, a pesar de sus importantes objetivos relacionados con la paz y la seguridad regionales e internacionales, no está orientado hacia los derechos humanos. No obstante, dado que en el Arreglo se establecen normas que conllevan la expectativa de un grado importante de aplicación y cumplimiento, los Estados participantes deben aprovechar ese valioso foro para imponer unas limitaciones a la transferencia de tecnologías de vigilancia que estén basadas en los derechos.

58. Para potenciar su papel en la elaboración de normas mundiales aplicables a la exportación, los Estados participantes podrían establecer un grupo de trabajo sobre derechos humanos que propusiera y analizara normas aplicables a la exportación que incorporasen las cuestiones de derechos humanos en las transferencias de tecnología. Con todo, independientemente de que se establezca ese grupo de trabajo u otro mecanismo de ese tipo, deberían desarrollar un marco en el cual la concesión de licencias sobre cualquier tecnología quede supeditada a un examen nacional de los derechos humanos y al cumplimiento por parte de las empresas de los Principios Rectores de las Empresas y los Derechos Humanos, como se analiza más adelante. Como afirma Privacy International, los Estados participantes, así como otros gobiernos exportadores, deben denegar la concesión de licencias "cuando exista un riesgo sustancial de que esas exportaciones puedan utilizarse para violar los derechos humanos, cuando en el destino no exista un marco jurídico que regule el uso de los elementos de vigilancia, o cuando el marco jurídico para su uso no esté a la altura de la legislación o las normas internacionales de derechos humanos"[70]. Para garantizar el cumplimiento cuando las licencias de exportación se denieguen con arreglo a esos criterios, las tecnologías de vigilancia en cuestión deben incorporarse a los regímenes de sanciones vigentes[71].

59. Si bien esas normas serían valiosas adiciones al Arreglo de Wassenaar, la capacidad del público o de determinadas organizaciones de la sociedad civil para supervisar su aplicación dependerá de que se establezcan obligaciones más estrictas en materia de transparencia en los planos nacional e internacional. El propio Arreglo debe promover esa transparencia estableciendo directrices claras y que puedan hacerse cumplir para el intercambio de información entre los gobiernos y la divulgación pública de información en relación con las normas de concesión de licencias, las decisiones de autorizar, modificar o rechazar las licencias, los incidentes o pautas de uso indebido de las tecnologías de vigilancia y las violaciones conexas de los derechos humanos, y el tratamiento de las vulnerabilidades digitales. En las leyes nacionales relativas a la exportación también deben asignarse recursos suficientes para el mantenimiento de registros públicos y la accesibilidad en relación con las decisiones de concesión de licencias de exportación, y debe ordenarse a los organismos gubernamentales pertinentes que soliciten contribuciones públicas y celebren consultas con los interesados cuando tramiten las solicitudes de licencias de exportación. Por último, los Estados también deben establecer puertos seguros para la investigación en materia de seguridad y eximir a los productos destinados al cifrado de las comunicaciones de las restricciones al control de las exportaciones[72].

[69] Véase Arreglo de Wassenaar, "IL - Israel cybersecurity export control policy" (presentación en PowerPoint), junio de 2016.

[70] Comunicación de Privacy International, pág. 8.

[71] *Ibid*., págs. 3 y 4.

[72] *Ibid*., pág. 5.

D. Aplicación por las empresas de los Principios Rectores sobre las Empresas y los Derechos Humanos

60. Dado el extraordinario riesgo de abuso que conllevan las tecnologías de vigilancia, la concesión de licencias de exportación debe prohibirse en la legislación de los países a menos que una empresa demuestre periódicamente que ha cumplido rigurosamente las responsabilidades que le incumben en virtud de los Principios Rectores con respecto al diseño, la venta, la transferencia o la prestación de servicios de asistencia de esas tecnologías. Eso serviría para convertir efectivamente los Principios Rectores en condiciones previas para que las empresas puedan operar en el mercado de los productos para la vigilancia. En informes anteriores, el Relator Especial ha explicado cómo el sector de la tecnología de la información y las comunicaciones debe cumplir su responsabilidad de respetar los derechos humanos (A/HRC/35/22, párrs. 45 a 75). Para que las empresas privadas de vigilancia puedan cumplir con esas responsabilidades, deben contar, como mínimo, con los siguientes elementos[73]:

a) Políticas de relaciones con el cliente en las que se reafirme inequívocamente la responsabilidad de las empresas de respetar la libertad de expresión, la privacidad y los derechos humanos en todas sus operaciones y que el cumplimiento del derecho internacional de los derechos humanos por parte del cliente es una condición para la aprobación y finalización de una venta, transferencia o contrato de asistencia;

b) Procesos de diligencia debida en materia de derechos humanos (como las evaluaciones del impacto en los derechos humanos) que se pongan en marcha cuando las empresas realicen actividades relacionadas con la libertad de expresión y la privacidad, como el diseño, la venta, la transferencia y la prestación de servicios de asistencia para productos y servicios de vigilancia;

c) Políticas internas y cláusulas contractuales estándar en las que se establezcan prohibiciones claras y específicas sobre la modificación personalizada de los productos, la selección de objetivos y la prestación de servicios de mantenimiento o asistencia que supongan una infracción del derecho internacional de los derechos humanos;

d) Procesos internos que garanticen que en las opciones de diseño e ingeniería se incorporen salvaguardias de los derechos humanos, como sistemas de aviso que detecten el uso indebido e interruptores que puedan activarse en caso de uso indebido;

e) Programas regulares de auditoría y procesos de verificación de los derechos humanos para asegurar que el uso de sus productos y servicios sea compatible con el derecho internacional de los derechos humanos, incluido el compromiso de divulgar públicamente las principales conclusiones de esas auditorías y procesos de verificación;

f) Procesos de notificación que ayuden a informar con prontitud sobre el uso indebido de sus productos a los órganos gubernamentales de supervisión pertinentes (como las instituciones nacionales de derechos humanos) o a los órganos intergubernamentales (como los mecanismos de presentación de quejas de los procedimientos especiales);

g) Informes de transparencia que revelen los posibles usos y capacidades de sus productos y los tipos de soporte posventa que se ofrecen, los incidentes de uso indebido y los datos relativos al número y tipo de ventas a organismos policiales o de inteligencia u otros organismos gubernamentales o a sus agentes;

h) Consultas periódicas con los titulares de derechos afectados, los grupos de la sociedad civil y las organizaciones de derechos digitales sobre los efectos observados o potenciales de sus productos y servicios y las salvaguardias de los derechos humanos necesarias para prevenir o mitigar esos efectos, haciendo especial hincapié en la participación de quienes corren el riesgo de sufrir discriminación o represión basada en la vigilancia, como las minorías raciales y étnicas y los grupos históricamente marginados;

[73] Muchas de esas normas se basan en las comunicaciones enviadas por la sociedad civil, que pueden consultarse en la adición al presente informe y en el sitio web del Relator Especial.

i) Mecanismos de reclamación que permitan a las personas presentar denuncias sobre abusos de los derechos humanos que se hayan visto facilitados por los productos y servicios de la empresa y proporcionen una evaluación independiente de esas denuncias y un seguimiento real;

j) Mecanismos de recurso que permitan a los denunciantes solicitar una indemnización, la presentación de disculpas u otras formas de reparación, según proceda, en los casos en que las denuncias se verifiquen de forma independiente.

E. Medidas corregulatorias

61. Los enfoques de los Estados y las empresas, tal como se describen aquí, pueden ser insuficientes para abordar el problema mundial de la vigilancia selectiva. También carecen de varias aportaciones importantes: las de los actores de la sociedad civil, ya sean activistas, tecnólogos, académicos, víctimas o incluso personas que pertenecen a más de una de esas categorías. La gobernanza corregulatoria, que implica una participación significativa de los agentes estatales, empresariales y de la sociedad civil, puede servir para diseñar un mecanismo de rendición de cuentas en materia de derechos humanos en el sector de la vigilancia privada. En particular, resultan instructivas las iniciativas de corregulación desarrolladas para inculcar el sentido de la responsabilidad y la necesidad de la supervisión entre las empresas del sector de la seguridad privada. Al igual que las empresas privadas de vigilancia, los riesgos que asumen las empresas privadas de seguridad están relacionados con su participación inherente en las funciones del Estado, en particular en el ámbito de la seguridad nacional. Por tanto, la corregulación de las empresas de seguridad privada exige que se haga un esfuerzo para informar a las empresas sobre las cuestiones delicadas preocupaciones en materia de derechos humanos y se ofrezcan incentivos para la participación de múltiples interesados (una certificación basada en procesos de auditoría y sistemas de supervisión en los que participe la sociedad civil), algo que puede ser muy útil para el sector de la vigilancia privada.

62. Hay dos aspectos del entorno normativo de las empresas de seguridad privada que merecen ser examinados en el contexto de las empresas privadas de vigilancia. En el Documento de Montreux sobre las obligaciones jurídicas internacionales pertinentes y las buenas prácticas de los Estados en lo que respecta a las operaciones de las empresas militares y de seguridad privadas durante los conflictos armados se esbozan algunas directrices en relación con las buenas prácticas de los Estados en esas situaciones[74]. Aunque no tiene carácter vinculante, contiene disposiciones derivadas del derecho internacional que obligan a las empresas de seguridad privada, así como recomendaciones en forma de prácticas óptimas para los Estados contratantes, los Estados territoriales y los Estados de origen. Sus principios de divulgación pública y diligencia debida son anteriores a las responsabilidades que se encuentran en los Principios Rectores y se reflejan en ellas.

63. El Código de Conducta Internacional para Proveedores de Servicios de Seguridad Privada también puede ser un modelo apropiado. Redactado con el apoyo de la sociedad civil, el sector privado y el Gobierno de Suiza, es uno de los pocos enfoques que cuenta con la participación de las empresas de seguridad privada. El Código de Conducta es una iniciativa de múltiples interesados en la que participan representantes de los Estados, las empresas de seguridad privada y las organizaciones de la sociedad civil. El Código de Conducta, que no tiene carácter vinculante, pretende ser un complemento de las actividades de seguimiento y supervisión y en él se articulan las obligaciones de las empresas derivadas del derecho internacional y se crea una estructura marco para la rendición de cuentas a la Asociación. La Asociación consta de una asamblea general, en la que están representados los grupos de interesados, y una junta directiva, que cuenta con 12 miembros electos que representan a los tres grupos de interesados. La pertenencia de una empresa a la Asociación

[74] Véase Suiza, Departamento Federal de Relaciones Exteriores, y Comité Internacional de la Cruz Roja, “Documento de Montreux sobre las obligaciones jurídicas internacionales pertinentes y las buenas prácticas de los Estados en lo que respecta a las operaciones de las empresas militares y de seguridad privadas durante los conflictos armados” (Berna, 2008).

está supeditada al cumplimiento del Código de Conducta, incluidos los procesos de certificación, auditoría y verificación.

64. Como se establece en los estatutos, la idea que sustenta el Código de Conducta es promover el uso responsable de los servicios de seguridad privada, así como el respeto del derecho internacional de los derechos humanos. En el propio Código de Conducta se esbozan los compromisos generales de los Estados y las empresas de seguridad privada y otros proveedores de servicios de seguridad privada, así como los principios de conducta específicos en esferas como el uso de la fuerza, el encarcelamiento, la detención de personas, la tortura y otros castigos, la violencia por motivos de género, la trata de personas, la esclavitud y el trabajo forzoso, la discriminación, y la identificación y registro del personal de seguridad privada[75].

F. Nuevo enfoque de las Naciones Unidas para las prácticas de vigilancia

65. El Consejo de Derechos Humanos ha creado varios grupos de trabajo encargados de abordar temas clave sobre la aplicación de las normas internacionales de derechos humanos, lo que ha supuesto un gran avance. El Consejo o sus procedimientos especiales podrían considerar la posibilidad de establecer un nuevo mecanismo para prestar a determinados casos un tipo de atención que los titulares de mandatos no pueden mantener y evaluar. Un nuevo grupo de trabajo, con un mandato transversal, o con un plan de acción concreto, podría prestar especial atención a las denuncias de interferencias de las prácticas nacionales de vigilancia —que afectan a muchas esferas del derecho de los derechos humanos y, por lo tanto, a muchos mandatos de procedimientos especiales— con los derechos humanos fundamentales.

V. Recomendaciones

66. **Dirigidas a los Estados:**

a) 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;

b) Los Estados que adquieren o utilizan tecnologías de vigilancia (“Estados compradores”) deben velar por que la legislación nacional permita su utilización únicamente de conformidad con las normas de derechos humanos relativas a la legalidad, la necesidad y la legitimidad de los objetivos, y deben establecer mecanismos jurídicos de reparación compatibles con su obligación de proporcionar un recurso efectivo a las víctimas de abusos relacionados con la vigilancia;

c) Los Estados compradores también deben establecer mecanismos que garanticen la aprobación, la supervisión y el control públicos o comunitarios de la adquisición de tecnologías de vigilancia;

d) Los Estados que exporten o permitan la exportación de tecnologías de vigilancia (“Estados exportadores”) deben velar por que los organismos gubernamentales competentes soliciten contribuciones públicas y celebren consultas con múltiples interesados cuando tramiten las solicitudes de licencias de exportación. Todos los registros relativos a los certificados de exportación deben conservarse y hacerse públicos en la mayor medida posible. Los Estados también deben establecer puertos seguros para la investigación en materia de seguridad y eximir a los productos destinados al cifrado de las comunicaciones de las restricciones al control de las exportaciones.

[75] Véase también la comunicación de Sarah McKune, pág. 10.

e) Los Estados exportadores deben adherirse al Arreglo de Wassenaar y respetar sus reglas y normas en la medida en que sean compatibles con el derecho internacional de los derechos humanos;

f) Los Estados participantes en el Arreglo de Wassenaar deben desarrollar un marco en el que la concesión de licencias sobre cualquier tecnología quede supeditada a un examen nacional de los derechos humanos y al cumplimiento por parte de las empresas de los Principios Rectores de las Empresas y los Derechos Humanos. De la elaboración de ese marco podría encargarse un grupo de trabajo sobre derechos humanos establecido a tal efecto. Además, deben establecer directrices claras y que puedan hacerse cumplir sobre la transparencia y la rendición de cuentas con respecto a las decisiones de concesión de licencias, los abusos de los derechos humanos relacionados con la vigilancia y el tratamiento de las vulnerabilidades digitales.

67. **Dirigidas a las empresas:**

a) Las empresas privadas de vigilancia deben reconocer públicamente su responsabilidad de respetar la libertad de expresión, la privacidad y los derechos humanos conexos, e integrar los procesos de diligencia debida en materia de derechos humanos desde las primeras etapas del desarrollo de sus productos y durante todas sus operaciones. En esos procesos se deben tener en cuenta los derechos humanos mediante consideraciones en el diseño, la celebración de consultas periódicas con la sociedad civil (en particular con los grupos en riesgo de ser vigilados), y debe actuarse con una verdadera transparencia en la presentación de informes sobre las actividades empresariales que tengan un impacto en los derechos humanos;

b) Las empresas también deben establecer salvaguardias sólidas para garantizar que cualquier uso de sus productos o servicios se ajuste a las normas de derechos humanos. Entre esas salvaguardias figura la inclusión de cláusulas contractuales que prohíban la modificación personalizada de los productos, la selección de objetivos, la prestación de servicios de asistencia u otros usos que supongan una infracción de las normas internacionales de derechos humanos; la incorporación de características técnicas que puedan avisar del uso indebido, prevenirlo o mitigarlo; y la realización de auditorías y procesos de verificación de los derechos humanos;

c) Cuando las empresas detecten el uso indebido de sus productos y servicios para cometer abusos contra los derechos humanos, deben informar de ello sin demora a los órganos de supervisión nacionales, regionales o internacionales pertinentes. También deben establecer mecanismos eficaces de queja y de recurso que permitan a las víctimas de abusos de los derechos humanos relacionados con la vigilancia presentar denuncias y exigir reparación.

68. **Dirigidas a las Naciones Unidas: la Organización, en particular el Consejo de Derechos Humanos, debe crear un grupo de trabajo o un equipo de tareas con un mandato transversal encargado de supervisar y formular recomendaciones sobre las tendencias y los casos concretos de abusos de los derechos humanos que se hayan visto facilitados por la vigilancia digital.**

69. **Dirigidas a todas las partes interesadas: los Estados, el sector privado, la sociedad civil y demás partes interesadas pertinentes deben establecer iniciativas de corregulación orientadas a la elaboración de normas de conducta basadas en los derechos para el sector de la vigilancia privada y aplicar esas normas mediante auditorías independientes e iniciativas de aprendizaje y de políticas.**